ALGEBRA

BY

F. W. LEVI, DR. PHIL. NAT.
Hardinge Professor of Higher Mathematics
Calcutta University

VOLUME I

PUBLISHED BY THE
UNIVERSITY OF CALCUTTA
1942

BCU 1741

PRINTED IN INDIA

PRINTED BY KALIPADA MUKHERJEE
AT THE EKA PRESS, 210, CORNWALLIS STREET, CALCUTTA.

GS 3578

Reg. No. 69 O. P.

CONTENTS

Page

PREFACE ix

INTRODUCTORY REMARKS 1

0-1. Odd and even numbers 1

0-2. Mathematical induction 2

0-3. Permutations 2

0-31. Representation of permutations 2. 0-32. Composition o permutations 4. 0-33. Decomposition of permutations 5. 0-34. Even and odd permutations 6.

CHAPTER I. SYSTEMS OF LINEAR EQUATIONS .. 8

1-1. Introduction—A dialogue 8

1-2. n-vectors 13

1-3. Vectorspaces 14

1-4. Matrices. The method of "Sweep out" 17

1-5. Orthogonality. Homogeneous linear equations .. 20

1-6. Systems of non-homogeneous linear equations .. 23

1-7. The method of orthogonalisation 26

1-8. Determinants 29

1-9. The minors of a determinant 35

1-91; Generalised cofactors 38.

1-10. Solution of systems of linear equations by the help of determinants 40

1-(10)1. Comparison of the different methods for solving systems of linear equations 41.

1-(11). Linear transformations 43

1-(11)1. Composition of transformations. Product of matrices 44. 1-(11)11. n-vectors considered as matrices 45. 1-(11)12. Special matrices 46. 1-(11)2. Decomposition of matrices 46. 1-(11)3. The determinant of a matrix product 47. 1-(11)4. The inverse of a linear transformation 47.

CHAPTER II. FUNDAMENTALS OF GENERAL ALGEBRA .. 49

2-1. Principal Notions 49

2-11. Fundamental laws 49. 2-12. Modules 50. 2-13. Partition into classes 51. 2-14. Singular elements 53. 2-15. Operations in a module 54. 2-16. Rings 55.

Page

2-2. FIELDS 56

2-21. Nullelement and unitelement 56. 2-22. Homomorphism, isomorphism and automorphism 57. 2-23. The ring of classes of residues generated by a homomorphism 59. 2-24. Sub-fields of a field 62. 2-25. Primefields 63. 2-26. Fields of characteristic p 64. 2-27. Fields of characteristic 0 65. 2-28. Quotient fields 66. 2-29. Relation between a field and its subrings 68. 2-291. Identification 69.

2-3. POLYNOMIALS 72

2-31. Preliminary investigation 72. 2-32. Definition of a polynomial 73. 2-33. Rings of polynomials 74. 2-34. Commutative rings of polynomials 75. 2-35. Integral functions 76. 2-36. Polynomials in two indeterminates. Derivatives 77. 2-37. Homogeneous polynomials 79.

2-4. FACTORISATION 80

2-41. Fundamental notions 80. 2-42. Domains with factorisable elements 82. 2-43. Unique factorisations 83. 2-44. Euclidean domains 85. 2-45. The domain of the integral numbers 87. 2-46. Homomorphism modulo a prime-element 88. 2-47. Factorisation in $F[x]$ 88. 2-48. Factorisation in $D[x]$ 91. 2-49. Comparison between R and $R[x]$ 94.

2-5. THE FUNDAMENTAL THEOREM OF GENERAL ALGEBRA .. 95

2-51. Existence of a root in a suitable extension 95. 2-52. Extensions of F containing a root of $f(x)$ 96. 2-53. Factorisation of $f(x)$ into linear factors. General remarks 98.

2-6. EXTENSION OF A FIELD 100

2-61. Vectorspaces over a field 100. 2-62. Extension of the results of Chapter I to vectorspaces over an arbitrary field 102. 2-63. Finite extensions 103. 2-64. Rank of a field over a field 105. 2-65. Highest common factor and extension of a field 106. 2-66. Multiple roots 107. 2-67. Non-separable polynomials 108.

2-7. REPEATED EXTENSION OF A FIELD 109

2-71. Extension of a field to a ring and to a field by a finite number of steps 109. 2-72. Primitive element of an extension 110. 2-73. Extension by roots of two different irreducible polynomials 112. 2-74. Normal extension of a field 113. 2-741. Generalisations of the theorem on normal extensions 115. 2-742. Automorphisms of a normal extension 116.

CHAPTER III. GENERAL ALGEBRA, SPECIFIED THEORY 118

3-1. CYCLOTOMIC POLYNOMIALS 118

3-11. Reduction of the problem to the case when n is not divisible by the characteristic 118. 3-12. Primitive roots 119. 3-13. Cyclotomic polynomials of order n 121.

Page

3·2. GALOISFIELDS 121

3·21. Fundamental properties 121. 3·22. Automorphisms 124. 3·23. Calculation in a Galoisfield 125. 3·24. Application to the theory of numbers 127. 3·25. Application to finite geometries 128. 3·251. Application to statistical analysis 129.

3·3. THE FIELDS K(i) 130

3·31. The general case 130. 3·32. The field $R(i)$ 131. 3·33. A generalisation 134.

3·4. IRREDUCIBILITY OF POLYNOMIALS 135

3·41. A general method 135. 3·42. Reduction of the problem to the investigation of irreducibility in $D[x]$ 136. 3·421. Irreducibility in $R[x]$. 137. 3·43. Method of homomorphism 138. 3·431. Eisenstein's theorem 138. 3·432. A special case 139. 3·433. Irreducibility of the cyclotomic polynomials in $R[x]$ 139. 3·44. Irreducibility of determinants 141.

3·5. SYMMETRIC POLYNOMIALS 141

3·51. Elementary symmetric polynomials 141. 3·52. The main-theorem 143. 3·53. Alternating polynomials 145. 3·54. Symmetric rational functions 147. 3·55. Power-sums 147.

3·6. SOLUTION OF SPECIAL EQUATIONS BY RADICALS 148

3·61. Cubic equations 149. 3·62. Biquadratic equations 151.

3·7. RESULTANTS 152

3·71. Case when the coefficients of the highest term are equal to 1 154. 3·72. The general case 155. 3·73. Linear representation of a resultant 158.

3·8. CLOSED FIELDS 158

CHAPTER IV. CONTINUED FRACTIONS 161

4·1. GENERAL PROPERTIES OF CONTINUED FRACTIONS 161

4·11. Convergents of a continued fraction 162. 4·12. Finite continued fractions 165. 4·13. Proper and improper equivalence 167.

4·2. REPRESENTATION OF THE POSITIVE NUMBERS BY CONTINUED FRACTIONS 170

4·21. Correspondence between positive numbers and rational positive expansions 170. 4·22. Distribution of the continued fraction along the real axis 174.

4·3. PERIODIC CONTINUED FRACTIONS WITH INTEGRAL COEFFICIENTS 176

4·31. Expansion of quadratic elements into periodic continued fractions 177. 4·32. Purely periodic continued fractions 178. 4·33. Scheme for calculation 179. 4·34. Reduced quadratic numbers 182. 4·35. Expansion of square roots 183.

Page

4-4. APPLICATIONS TO THE THEORY OF NUMBERS 184

4-5. CONTINUED FRACTIONS WITH ELEMENTS $\phi(x)$ 185

4-51. The field B 186. 4-52. Expansion of the elements of B into continued fractions 189. 4-53. Approximation by rational functions 189. 4-54. Continued fractions whose elements are polynomials 191.

4-6. CONTINUED FRACTIONS WITH RATIONAL ELEMENTS.. .. 193

4-61. Convergence of continued fractions 194. 4-62. Tests of irrationality 195.

CHAPTER V. APPROXIMATION OF ROOTS 197

INTRODUCTION : ANOTHER DIALOGUE 197

5-1. HORNER'S SCHEME 202

5-11. Expansion of $f(x)$ as a polynomial in x-q 203. 5-12. Approximate calculation of roots by Horner's scheme 204. 5-13. A modification of Horner's scheme 206. 5-14. Lagrange's method 207. 5-15. Kakeya's theroem 210.

5-2. THE ROOTS OF REAL POLYNOMIALS 210

5-21. Real and complex roots 211. 5-22. Changes of sign 212. 5-221. Alterations of the first and the second kind 214. 5-222. Monotony of $C(b)$ 216. 5-223. Budan-Fourier's theorem 218. 5-2231. An example 219. 5-23 Sturm's theorem 220. 5-231. Legendre's polynomials 222. 5-24. Method for calculation of roots 224. 5-241. Linear interpolation 226. 5-242. Newton's method 226. 5-25. Poulain's theorem 227.

5-3. GRAEFFE'S METHOD 229

5-31. Real distinct roots 230. 5-32. Complex roots 232.

5-4. ROOTS OF COMPLEX POLYNOMIALS 236

5-41. Circles enclosing the roots of $\phi(x)$ 236. 5-42. Interconnection between the roots of a polynomial and those of its derivative 237.

5-5. INTERPOLATION 238

5-51. Lagrange's formula 239. 5-52. Interpolation by successive calculation 239. 5-53. Newton's formula 240.

CHAPTER VI. MATRICES 242

6-1. ADDITION AND MULTIPLICATION OF MATRICES OF DEGREE n 243

6-11. The group $G(\mathrm{K}, n)$ 246. 6-12. The ring $R(\Delta)$ 247. 6-13. Notations and formulas 249.

6-2. TRANSFORMATION OF VECTORSPACES 251

6-21. Permutations as linear transformations 254.

Page

6-3. THE CHARACTERISTIC POLYNOMIAL OF A MATRIX 259

6-31. Characteristic polynomials with n different roots 261. 6-32. Multiple roots of a characteristic polynomial 262. 6-33. Transformations with characteristic polynomial $(\lambda - x)^r$ 266. 6-331. The case r′=1 269. 6-332. The case r′=r 270. 6-333. Characteristic polynomials with a single root : general case 271. 6-34. Characteristic polymonials with any number of roots 273. 6-341. Application to the theory of the linear substitutions of a complex variable 274. 6-35. Polynomials of which A is a root 275.

6-4. ELEMENTARY DIVISORS 276

6-41. Congruent matrices 277. 6-42. "Sweep-out" for matrices of $R(\Delta, n)$ 279. 6-43. Congruence by matrix multiplication 283. 6-44. The ring $R(K[x], n)$ 284. 6-45. The ring $R(J, n)$ 286.

6-5 MATRICES AND FORMS 288

6-51. Unitary matrices 288. 6-511. Orthogonal matrices 292. 6-52. Symmetric and antisymmetric matrices 293. 6-53. Hermitean matrices 294. 6-54. Hermitean and quadratic forms 296. 6-541. The law of inertia for quadratic forms with real coefficients 298. 6-542. Applications to Geometry 299. 6-55. Bilinear forms with contragradient indeterminates 300.

INDEX 301

CORRECTIONS 305

PREFACE

This book has been written for the use of Indian students ; it covers a portion of the Post-Graduate Pure Mathematics course of the University of Calcutta. The interest in modern algebra has much increased all over India in recent years, but the lack of a textbook in the English language made it difficult to introduce the subject in the regular courses. The author expects that this book will help to enhance the popularity of algebra at Indian Universities, and the encouragement which he received from friends in U.S.A. makes him hope that the new textbook will be useful even outside India.

The urgent need for a book of this kind was felt first when a new course in algebra was introduced in Calcutta 1936. The students were not able to follow the lectures without some kind of textbook in their hands. Thus it was necessary to issue lecture-notes* in small instalments which were printed by the University Press as quickly as possible. In spite of many small deficiencies due to the circumstances under which those lecture-notes were published, they could be used as a basis for the instruction in algebra in the Post-Graduate Department of Pure Mathematics of our University during six academic years. The present book can therefore be considered as a second edition, completely revised in accordance with the experience obtained by the teaching.

I am much indebted to two lecturers who did most of the teaching in algebra during the last few years, Dr. Rabindranath Sen and Mr. Rajchandra Bose, M.A. for letting me participate in the experience which they obtained by lecturing to general and tutorial classes according to those lecture-notes. During the last session, typed copies of the present book where already in the hands of those scholars, and many small alterations were made on their advice. I had also much benefit from conversations with students, especially those who after having completed the course continued to study mathematics as research scholars under my guidance ; they remembered very well the passages of the lecture-notes which used to be most difficult to them. Although modern algebra is not a difficult subject, it requires some change of mind from students whose previous training was in classical mathematics only. They are familiar with investigations on interesting mathematical entities, but they are not used to considerations about relations between objects which are indeterminate. No wonder that the students felt uneasy when the course was introduced ; they did not realise the "raison d'etre" of the subject. Gradually, bewilderment gave way to enthusiasm, especially among the better students ; when the first two-years course was completed, some of them suggested to me to omit—or at least restrict—such subjects as continued fractions and approximation of roots, and to give more of modern algebra, but I was unable to follow this advice.

---

* Algebra, lectures delivered to post-graduate students, Part I-V, by F. W. Levi 1936-37.

It was the author's intention to keep an equal balance between modern and classical portions of algebra ; he imposed on himself the greatest restriction in the use of notions and notations of more recent origin, and he limited his programme on general algebra by keeping the notions of ideal and of non-commutative group outside. These subjects will be treated in the second volume. Actual teaching-experience made him modify this plan ; one will find in this book some notations like : integral domain, Euclidean domain etc., which have not been used in the lecture-notes, but which proved very useful in the class. The self-imposed limitations concerning theory of groups have been shown to be too rigid. The general notion of group is an essential part of every reasonable teaching of geometry ; by this argument, the author's junior friends and disciples convinced him that no additional burden would be imposed on the students by including this notion in the compulsory algebra-course.

In a systematical representation of the subject (e.g. van der Waerden's "Moderne Algebra") one starts from those notions which have been proved to be fundamental ; when the whole system has been built up, one sees the reasons for every step, and one feels much admiration. A methodical discussion starts with examples, the notions being introduced successively at those points where their usefulness becomes obvious. In this respect too, the author follows a middle way. Chapter I deals with the solutions of systems of linear equations. The importance of this problem is obvious ; the results are applied in the course on geometry which the students as a rule follow during the same session. Since the introduction of new notions like vector, vectorspace etc., is shown to be very helpful, the reader may get the necessary confidence to dive into the very abstract investigations of Chapter II which find their applications in Chapter III. These considerations on general algebra are continued in Chapter VI where matrices are studied. The Chapters IV and V deal with continued fractions and with approximative calculations. It is possible to treat all classical problems from the point of view of general algebra. Of course one can consider the field of the real numbers as a special case of the formally real fields ; a substantial portion of the continuum-algebra can be shown to hold in these fields. The notion of formally real fields has not been used in this book ; the author has preferred to respect the autonomy of the theory of numerical calculation. This theory originates from the needs of the computor, and it has been treated here accordingly—starting from a very simple principle of calculation, Horner's scheme. Whereas in the fifth chapter very little reference is made to the principles of general algebra, the continued fractions (Chapter IV) are treated so to say in a half-classical manner. It appears that the suppositions which are usually made in this theory are not all necessary, and that they afford interesting generalisations. This kind of treatment has been suggested to the author, not by papers on general algebra, but by a book on numerical calculation (Runge-Koenig).

Some readers may be astonished to find two dialogues in this book. Needless to say that the two characters—tutor and student—do not represent any ndividuals ; nor is the "student" a true picture of the average Indian mathematics student of the present time. He is an international creature, and some of the remarks originate from the difficulties which the author himself had to face when a student more than 30 years ago. There are certain items in mathematics which can best be made clear by a frank discussion ; the author wants to encourage this form of teaching by giving these two specimens of discussions between a teacher and his pupil. The "introductory remarks" (Chapter zero) are meant to refresh the memory of a few subjects which are supposed to be known by the students joining the post-graduate classes.

Western mathematicians may wonder why the "method of identification" is discussed here in such an explicit manner. This item which was not treated in the lecture-notes has been introduced into the book because the experience of teaching showed its necessity. This is the only occasion where I came across an essential difference between the Indian way of thinking in mathematics and the western one. It seems that the western mind performs so to say automatically the operation of identification ; even Edmund Landau whose rigour and explicitness have become proverbial used to pass it over without explanation. I remember only a single case where I had to discuss this item with a student of Leipzig University, and at that occasion it was not my task to clear up the difficulty, but to show that there is one. When introducing the new course on algebra in Calcutta I did not like to burden it with considerations which in Europe were thought to be unnecessary sophisteries, and I was very astonished that every year, the students felt difficulties and asked for explanations at that particular point. I am stating this experience here without feeling competent to explain it. Scholars on Indology may find some clue in ancient Indian logic —though very few of our mathematics students have an explicit knowledge of it. Similarly, I must leave it to Indian scholars to explore why western people fail to recognise a difficulty which is so obvious even to an average mathematics student in this country.

In offering this book to the public, I have much pleasure to thank for their generous help the authorities of the University of Calcutta: the Senate, the Syndicate and the three Vice-chancellors who were in charge of the University since the publication of the lecture-notes was undertaken in 1936. In particular I am obliged to the President of the Council of Post-Graduate Teaching in Arts, the Hon'ble Dr. Shyama Prasad Mookerjee for his kind understanding and his energetic support without which it would not have been possible to bring out this book in an adequate form during the present emergency.

The assistance which I received from lecturers and research-scholars of the Department of Pure Mathematics has already been gratefully acknowledged. One of them, Bankim Chandra Chatterjee, M.Sc. must be mentioned especially for having assisted the author in the correction of the proof-sheets from beginning to end. The Eka Press has printed the book with great care and ability.

Binsar (Himalya),
June 1st. 1942.

F. W. LEVI

INTRODUCTORY REMARKS

0·1. *Odd and even numbers.*

The notions "odd" and "even" apply to positive as well as to non-positive integral numbers, though they were used originally for positive ones only. A number which is the double of an integral number is said to be *even*. A non-even integral number is *odd*. Hence zero is even ; if a is even (odd), $-a$ is even (odd) and $a\pm 1$ is odd (even). The integral numbers form a double sequence where the elements are alternately even and odd. The distinction between even and odd—though it involves a very simple principle—plays an important role in Algebra and in other branches of Mathematics.

The sum as well as the differences of two odd (even) numbers are even ; the sum and the difference of one odd and one even number are odd. To generalise these propositions, consider

$$M = \sum_{j=1}^{n} m_j. \tag{1}$$

Let q terms of the sum be odd, and the remaining $n-q$ terms be even numbers.

Put $\qquad m_j = 2r_j + 1 \qquad$ if m_j is odd

$\qquad\qquad m_j = 2r_j \qquad$ if m_j is even ; then

$$M = \sum_{j=1}^{n} 2r_j + q \tag{2}$$

is odd or even according as q is odd or even. I.e.

If in a sum of integral numbers exactly q terms are odd, the sum is odd or even, according as q is odd or even.

In particular, put $q=n$.

A sum of n odd numbers is odd or even, according as n is odd or even.

Exercise. Let m objects be arranged in a linear manner, and let them be rearranged to a second position. Hereby a objects move forward to the right whereas b objects recede to the left. Out of the a elements moving forward, a_1 are moved by an even number of places, a_2 by an odd number. Similarly b_1 objects recede by an even and b_2 by an odd number of places. Prove that a_2 and b_2 are either both odd, or both even.

0·2. *Mathematical induction.*

In life as well as in experimental Science one uses to make conclusions in the following manner. A certain observation is made in a large number of particular cases, and from these statements one concludes that there exists a general rule. This form of conclusion is called "conclusion by induction". A statement as e.g. "Palm trees grow higher than bananas" is based on an experience got from a restricted number of plants of both the species. We shall not investigate here why conclusions of this type are justified in many cases. In mathematics, ordinary induction is not admissible*. To attain general rules, a form of conclusion is often applied which for its apparent similarity with ordinary induction is called : "*mathematical induction*".

Principle of mathematical induction. Let $S(n)$ be a statement concerning the positive integral numbers $n = 1, 2, \ldots$, and : (1) let $S(1)$ be a true statement ; (2) let it be possible to demonstrate that if $S(m)$ is a true statement, then $S(m+1)$ is also a true statement, then $S(n)$ holds for every positive integral value of n.

Proof. Let $S(n)$ be not true for every positive integral value, then there exist positive integral values for which the statement does not hold. Among these values there is one smallest integral number, say $a+1$. As $S(1)$ is supposed to hold, a is a positive number. Thus $S(a)$ holds, but $S(a+1)$ does not hold contrary to the supposition (2) ; hence $S(n)$ holds for every positive integral value of n.

Corollary. If $S(n)$ is true for $n = n_0$, and if supposition (2) of the above proposition holds, then $S(n)$ holds for $n \leqq n_0$.

0·3. *Permutations.*

0·31. *Representation of permutations.* Given n distinct objects, say

$$1, 2, \ldots, n. \tag{1}$$

Consider the transformations by which the objects (1) are interchanged. These transformations are called *permutations*. Any permutation is uniquely determined when it is known into which element each individual element of (1) is transformed. Hence a permutation can be represented by the help of two lines, each of them containing the n elements (1), ordered in such a way that below every element, say k, in the upper line is written the element a_k into which k is transformed.

---

*As a matter of fact the task of mathematics does not consist mainly in the enunciation of statements, but in showing the logical necessity of these statements. A mathematical statement based on ordinary induction may be true, but it is of little mathematical value, unless it gets a logical foundation. An example of an obviously false statement attained by induction is this : "The number 2520 is divisible by every integral number". Of course it is divisible by 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and by some more numbers which may have been taken at random, say 20, 56, 126, 420, 630 ; thus one may falsely conclude the truth of the statement by induction.

$$A = \begin{pmatrix} 1, & 2, & \ldots, & k, & \ldots, & n \\ a_1, & a_2, & \ldots, & a_k, & \ldots, & a_n \end{pmatrix} = \begin{pmatrix} k \\ a_k \end{pmatrix}. \tag{2}$$

It is not necessary that the digits (1) are given in their natural order in the first line of the scheme (2). They may be interchanged in any manner if the same change is made in the second line; the only essential thing is that a particular element a_k is put below a particular k to signify that k has to be replaced by a_k. To check whether two given permutations given in any manner are identical or not, one may interchange the vertical columns in the corresponding schemes (2) in such a way that the digits in the first lines have the natural order in both the cases. If after this operation the second lines are the same for the two permutations, these are identical, otherwise different. It is however not always convenient to arrange the digits of the first line in their natural order. E. g. there exists to every permutation A an inverse permutation

$$A^{-1} = \begin{pmatrix} a_1, & a_2, & \ldots, & a_k, & \ldots, & a_n \\ 1, & 2, & \ldots, & k, & \ldots, & n \end{pmatrix} = \begin{pmatrix} a_k \\ k \end{pmatrix}. \tag{2'}$$

The connection between A and A^{-1} is such that if the permutation A replaces any object c by an object d, then A^{-1} replaces d by c. Hence if one interchanges the objects (1) at first according to A and then according to A^{-1}, as a result every object remains unaltered. The permutation not altering any object must indeed also be considered as a permutation; it is called the *identical permutation*, or the *identity*.

$$J = \begin{pmatrix} 1, & \ldots, & k, & \ldots, & n \\ 1, & \ldots, & k, & \ldots, & n \end{pmatrix} = \begin{pmatrix} k \\ k \end{pmatrix}. \tag{3}$$

Furthermore, the following permutations are of special interest:

Cyclic permutations:

$$\begin{pmatrix} a_1, & \ldots, & a_{m-1}, & a_m, & b_1, & \ldots, & b_{n-m} \\ a_2, & \ldots, & a_m, & a_1, & b_1, & \ldots, & b_{n-m} \end{pmatrix} = (a_1, \ldots, a_m); \tag{4}$$

in particular cyclic permutations with $m = 2$ are called *transpositions*.

$$\begin{pmatrix} a, & b, & c_1, & \ldots, & c_{n-2} \\ b, & a, & c_1, & \ldots, & c_{n-2} \end{pmatrix} = (a, b). \tag{5}$$

The transposition (5) is therefore only an interchange of the two objects a and b ; the notations on the right hand side of (4) and (5) will be generalised in 0·33.

0·32 *Composition of permutations.* Consider 3 permutations of the objects 0·31, (1) say

$$A = \begin{pmatrix} k \\ a_k \end{pmatrix}, \quad B = \begin{pmatrix} k \\ b_k \end{pmatrix}, \quad C = \begin{pmatrix} k \\ c_k \end{pmatrix}.$$

As a_k takes all the values $1, \ldots, n$, one can also denote

$$B = \begin{pmatrix} a_k \\ b_{a_k} \end{pmatrix}.$$

If one performs therefore *at first* the permutation A, and *then* the permutation B, any object k is replaced by b_{a_k}.

The permutation attained in this manner is said to be *composed* of A and B and will be denoted here as a *product*

$$BA = \begin{pmatrix} k \\ b_{a_k} \end{pmatrix}. \tag{1}$$

The products B A and A B are in general different. Readers may wonder why the order of the transformations appears in the notation of the product written from the right to the left. This manner of notation has its analogues in other branches of mathematics, e. g. $\phi\, f(x)$ means that x should be represented by $y = f(x)$, and then y by $\phi(y)$. For this similarity, the notation used here is sometimes called a "functional" manner of notation. Many authors use an inverse method of notation proceeding from the left to the right. It is a mere convention which notation to follow, as both ways of notation are equivalent and have their (purely formal) advantages and disadvantages.

Applying formula (1) to the products CB, (CB)A, C(BA), one gets

$$\begin{pmatrix} k \\ c_{b_{a_k}} \end{pmatrix} = (CB)A = C(BA). \tag{2}$$

Hence one can omit the brackets on the right hand side, and denote (2) by C B A. This permutation is attained by performing at first A, then B, and finally C. From (2) follows :

For the composition of permutations the associative law holds.

Applying (2) to (2′) and (3) of 0·31, one gets for every permutation A

$$AJ = JA = A \tag{3}$$

$$AA^{-1} = A^{-1}A = J. \tag{4}$$

Let furthermore A and B be any two permutations, and

$$AX = B, \quad YA = B\,; \tag{5}$$

by multiplying A^{-1} from the left (right) hand side and applying (2) and (4) one gets

$$X = A^{-1}B, \; Y = BA^{-1}. \tag{6}$$

On the other hand (6) is a solution of (5), thus the equations (5) possess one and only one solution.

0·33. *Decomposition of permutations.* A permutation can be represented as a product of permutations of a special type. Two important ways of representation will be discussed here.

Theorem 1. Every permutation of $n > 1$ objects can be represented as a product of transpositions.

Proof. (By mathematical induction) For $n = 2$ the theorem is obvious. Suppose the theorem to be true for $n = m - 1$, then it holds also for those permutations of m objects where at least one object remains unaltered. Let A be an arbitrary permutation of m objects, and let by A, the object a be changed into b. Then a is unaltered by $A' = (a, b)\,A$, and therefore A' is a product of transpositions. Hence

$$A = J\,A = (a, b)\;(a, b)\;A = (a, b)\;A'$$

is a product of transpositions.

Exercises. (1) Prove that the number of the different permutations of n objects is equal to $n\,!$

(2) Represent J as a product of two transpositions.

(3) Show that $A \neq J$ can be represented as product of transpositions which are less than n in number.

The representation of A as a product of transpositions is not unique. One can *e.g.* perform any number of transpositions and then arrange systematically (see ex. 3). We shall now consider a different representation which is unique.

Let A be any particular permutation, and let a_1 be transformed by A into a_2, again a_2 into a_3 etc. The sequence

$$a_1, a_2, a_3, \ldots$$

is infinite, every element in it determines uniquely the following as well as the preceding one, hence —as it contains only a finite number of different elements — it is a periodic sequence. The elements, say

$$a_1, a_2, \ldots, a_{m_1} \tag{1}$$

are interchanged among themselves in a *cyclic* order. Let b_1 be any object subject to the permutation and not belonging to the cycle (1), then b_1 is transformed into an element b_2, which does not belong to (1), and so b_1 generates a cycle $b_1, \ldots, b_{m_2}$ which has no element in common with (1). This procedure can be repeated till it stops after $r \leqq n$ steps. The permutation therefore generates a partition of the given objects into r cycles

$$(a_1, \ldots, a_{m_1}) \ldots (d_1, \ldots, d_{m_r}), \tag{2}$$

where $$1 \leqq r \leqq n.$$

In every cycle the order of the elements is determined up to a cyclic permutation which remains arbitrary, and the cycles can be interchanged among themselves but for a given A, every object determines its cycle uniquely; hence A determines (2) uniquely. The objects which are not displaced by A form cycles by themselves each. For abbreviation, those cycles with one element only are often omitted. The notation introduced in 0-31, (4) and (5) appears now to be a special case of the notation introduced here. On the other hand, (2) can be considered as a product of the cyclic permutations corresponding to its cycles. Hence:

Theorem 2. Any permutation A can be represented as a product (2) of cyclic permutations in such a way that different factors displace different objects. This representation is unique except for the order of the factors which remains arbitrary.

0·34. *Even and odd permutations.*

Definition. The permutation A is said to be even or odd according as the number of *even* cycles in 0-33, (2) is even or odd.

Theorem. Every product of an even (odd) number of transpositions is even (odd).

Proof. The theorem is obvious if the number of the transpositions is zero or one. By the principle of mathematical induction one has therefore only to prove that by composition of a permutation A from the left with a transposition, an even A becomes odd and conversely. Let A be represented by cycles as in (2) the cycles with one element only (if any) also being considered, and let (a_1, b_1) be the transposition. Then either a_1 and b_1 occur in the same cycle of A, or in two different cycles. Now

$$(a_1, b_1)\ (a_1, \ldots, a_r,\ b_1, \ldots, b_s) = (a_1, \ldots, a_r)\ (b_1, \ldots, b_s).$$

Multiplying from the left with (a_1, b_1) and interchanging the two sides one gets

$$(a_1, b_1)\ (a_1, \ldots, a_r)\ (b_1, \ldots, b_s) = (a_1, \ldots, a_r,\ b_1, \ldots, b_s).$$

As the other cycles are unaltered, the left hand factor (a_1, b_1) effects either a partition of a cycle into two cycles, or conversely an amalgamation of two cycles into one. An odd cycle is partitioned into one even and one odd, an even cycle into either two odd or two even ones. Hence the number of even cycles changes by ±1. Similarly for the amalgamation as it is the converse operation.

Corollary (1). A permutation which can be represented as a product of an even (odd) number of transpositions cannot be represented as a product of an odd (even) number of transpositions.

Corollary (2). By composing two even (odd) permutations one gets an even permutation; by composing one even and one odd permutation one gets an odd permutation.

Exercises. (1) Write down some permutations, and investigate whether they are even or odd.

(2) Show that every even permutation of $n > 2$ objects can be represented by composing suitable cyclic permutations of 3 objects each.

(3) An even cycle is an odd permutation, an odd cycle is an even permutation.

CHAPTER I

In this chapter systems of linear equations

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = a$$
$$b_1 x_1 + b_2 x_2 + \ldots + b_n x_n = b$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$k_1 x_1 + k_2 x_2 + \ldots + k_n x_n = k$$

will be considered.

1·1. *Introduction — A dialogue.*

Student. The problem enunciated at the beginning of this chapter seems to be a very easy one, but I have seen such words as "vectorspace", "rank", "matrix" later in the book ; I also noticed determinants and formulas with upper and lower indices. I cannot understand why the author is trying to make a very simple thing so complicated. The problem can be solved with the help of methods which I learned, when I read for the matriculation examination.

Tutor. Of course, it is my duty to help you to understand this theory clearly, but Mathematics is not a matter of seniority. History shows several examples where mathematicians were superior to their masters at a very early age of life. I should not miss the opportunity to learn something from you ; please, explain your solution of the problem.

Student. It is simply the method of substitution ! From the last equation it follows that $x_n = (k - k_1 x_1 - \ldots - k_{n-1} x_{n-1}) : k_n$. Putting this value into the remaining linear equations, I get linear equations with $n - 1$ unknown only. After having solved this system, we calculate the value of x_n by putting the values of $x_1, \ldots, x_{n-1}$ in that equation. Is it so ?

Tutor. Yes — provided $k_n \neq 0$.

St. In the case $k_n = 0$, x_n is infinite !

T. I do not think so ! — E. g. consider two equations and $n=2$, $k_2 = 0$, say

$$x_1 + 2x_2 = 5, \quad x_1 + 0x_2 = 1.$$

The only solution of this system is obviously $x_1=1$, $x_2=2$.

St. Yes, that is true.— If $k_n=0$, then I take another equation of the system in place of the last one. Thus without loss of generality, I suppose $k_n \neq 0$. I think you will be satisfied.

T. Unless the coefficient of x_n is zero in each equation of the system.

St. In this case the system has to be considered as a system with $(n-1)$ variables only; it would be absurd to consider it as a system of n variables as the equations are actually independent of x_n.

T. Perhaps less absurd than you may believe, but I accept your definition that a system of linear equations should be considered to depend on such variables only, as have at least one coefficient different from zero.

St. Certainly.

T. After x_n has been eliminated, how do you continue?

St. I shall repeat the process again and again until I get one equation with one variable x_1, and then there is no problem left.

T. You suppose that the number of equations is equal to the number of the variables, and you believe that at every step of your procedure, both the numbers decrease by exactly one?

St. Certainly, but the number of the equations may also be less than the number of the variables, let us say $m < n$ equations in n variables. In this case one puts the terms with $x_{m+1}, \ldots, x_n$ to the right hand side. These variables may take arbitrary values. For every set of values $x_{m+1}, \ldots, x_n$, there exists one solution $x_1, \ldots, x_m$, as there are as many of these variables, as there are equations. The number $n-m$ is the *degree of freedom* of our system, as the values of $n-m$ variables may be chosen arbitrarily.

T. And if there are more equations than variables?

St. Then there cannot exist any solution. It is obvious that n variables cannot satisfy a system of more than n conditions.

T. But it seems to me that the system $x=1$, $2x=2$ has a solution although it is a system of two equations with one variable.

St. But these equations are not different. Equations which differ by a common factor only cannot be considered as different, and it is common sense to consider only such equations which are different.

T. Thus, if two equal equations are given, one of them should be dropped.

St. Yes.

T. But this must be done also at the later stages of the procedure.

St. I cannot follow you exactly.

T. Consider :

$$\begin{aligned} 7x_1-38x_2+3x_3&=13\\ 3x_1+13x_2+2x_3&=17\\ 2x_1-\ 5x_2+\ x_3&=\ 6 \end{aligned}$$

3 different equations in x_1, x_2, x_3. Since the degree of freedom is zero, do you expect to get exactly one solution ?

St. Yes ! Put $x_3=6-2x_1+5x_2$ in the first two equations, then

$$\begin{aligned} x_1-23x_2&=-5\\ -x_1+23x_2&=\ \ \ 5. \end{aligned}$$

T. These equations differ by a factor -1 only ; hence one of them must be dropped. Thus you may choose x_2 in an arbitrary manner. Put $x_1=23\,x_2-5$, $x_3=-41x_2+16$, and this will solve the system of equations for every value of x_2. You have one "degree of freedom", although the number of the equations is equal to the number of the variables.

St. That is true. This example is obviously a wicked exception.

T. You may call it an exception if you like, but there are plenty of them.

St. I see !—There may be certain cases, where the degree of freedom is higher than the difference between the number of the variables and the number of the equations, but at any rate n equations with n variables have at least one solution which can be found by the method of substitution.

T. Why ?

St. Because the number of the equations can decrease, as one may get two equal equations by the procedure of substitution, and then one of them must be dropped, but the number of the variables cannot.

T. Try :

$$\begin{aligned} 9x_1-15x_2-3x_3&=13\\ 3x_1+10x_2+2x_3&=\ 1\\ 2x_1-\ 5x_2-\ x_3&=\ 2. \end{aligned}$$

St. Substitute $x_3 = 2x_1 - 5x_2 - 2$ in the first and in the second equation.

Hence

$$3x_1 = 7$$

$$7x_1 = 5. \quad \text{This is funny.}$$

T. Indeed, the coefficients of x_2 in both the equations became zero; thus the equations have to be considered as equations of one variable only. Now x_1 should be equal to 7:3 and to 5:7; that is impossible.

St. Perhaps I was somewhat rash in conceding that a system of equations in n variables should be considered as a system in $(n-1)$ variables if the coefficients of one of the variables are all equal to zero. Let us retain x_2 and put

$3x_1 - 0x_2 = 7$

$7x_1 + 0x_2 = 5$. Hence $x_1 = \frac{5}{7} - 0x_2$, and therefore $0x_2 = 34:7$, $x_2 = \infty$.

T. What do you mean by ∞?

St. Infinity! That is a number which is greater than every other number and equal to 1:0.

T. Can you calculate with this ∞ as with an ordinary number?

St. Certainly.

T. Then $-\infty = -1:0 = 1:(-0)$ and for $-0 = 0$, $-\infty = \infty$ holds. Hence $0 = 2\infty$, and therefore $0 = \infty$.

St. No, that is not so. One cannot calculate with this symbol as with an ordinary number. But, as a matter of fact, this ∞ occurs in mathematics. It is a somewhat complicated matter, one needs differential calculus to handle it, and I was hoping that you may explain it to me clearly one day.

T. On another occasion. The symbol ∞ does occur; sometimes it is used rightly, sometimes wrongly; use and misuse, both are found in textbooks. Considering systems of linear equations, we enquire about those numbers which taken for $x_1, \ldots, x_n$ respectively, satisfy those equations. Numbers can be added, subtracted and multiplied; one can also divide a number by a number, unless the divisor is zero. The division by zero is meaningless as far as numbers are concerned.

St. And the example which I attempted just before ?

T. It has no solution, since x_1 cannot simultaneously be equal to 7:3 and equal to 5:7.

St. So there exist systems of 3 equations in 3 variables which have no solutions, systems which have an infinity of solutions, and systems which have exactly one solution. How did you construct those examples by which you cornered me ?

T. It is not difficult if one knows a little bit of the theory.

St. Those vectorspaces, matrices, rank etc. ?—Sir, I should be thankful if you could explain to me some portion of the theory without using those notions. I do not like those innovations.

T. Then try the simplest case : $ax = b$.

St. Then $x = b:a$.

T. Provided $a \neq 0$.

St. If $a = 0$, $b \neq 0$, the equation has no solution as there exists no number x, for which $0x = b \neq 0$. If however $a = 0$, $b = 0$, then every value x is a solution.

T. Indeed !—This simple case is the seed of the whole theory.

Now try

$$a_1x + a_2y = a$$
$$b_1x + b_2y = b.$$

St. $\Delta y = \Delta_1$, $\Delta x = \Delta_2$, where $\Delta = a_1b_2 - b_1a_2$, $\Delta_1 = a_1b - b_1a$, $\Delta_2 = ab_2 - ba_2$. If $\Delta \neq 0$, then $x = \Delta_2 : \Delta$, $y = \Delta_1 : \Delta$.

T. In this case there exists no other solution, and these values satisfy the given equations, as you may verify easily.

St. If $\Delta = 0$, but Δ_1 or Δ_2 is different from zero, there is no solution. If $\Delta = \Delta_1 = \Delta_2 = 0$, then every couple of values (x, y) satisfies the equations.

T. Consider $x + 2y = 5$, $3x + 6y = 15$. Here $\Delta = \Delta_1 = \Delta_2 = 0$, but e.g. $(x, y) = (0, 0)$ is not a solution, as $x = 5 - 2y$.

St. This is true, but I cannot understand it. The equations $\Delta x = \Delta_2$, $\Delta y = \Delta_1$ are satisfied by every pair of values x, y if $\Delta = \Delta_1 = \Delta_2 = 0$.

T. These equations are consequences of the given equations; they are *necessary* conditions for solutions x, y of the given systems but they may not be *sufficient* ones. The case $\Delta = \Delta_1 = \Delta_2 = 0$ contains different cases. (1) If all the coefficients are equal to zero, then every pair (x, y) is a solution. (2) Let $a_1 = a_2 = b_1 = b_2 = 0$, but $(a, b) \neq (0, 0)$ then there is no solution. (3) Let at least one of the 4 coefficients on the left side be $\neq 0$. Without loss of generality, $a_1 \neq 0$. Put $b_1 : a_1 = \lambda$.

Hence
$$0 = \Delta = a_1(b_2 - \lambda a_2),\ b_2 = \lambda a_2$$
$$0 = \Delta_1 = a_1(b - \lambda a),\ b = \lambda a.$$

$(b_1 x + b_2 y - b) = \lambda\ (a_1 x + a_2 y - a)$. Hence $x = (a - a_2 y) : a_1$ for arbitrary y furnishes all the solutions. There are therefore 5 different cases.

St. For a higher number of variables and of equations a full analysis may become very complicated. How to tackle the problem for an arbitrary n?

T. For this, I propose to you to study the notions of vectorspace, rank, matrix, determinant etc., as explained in the following articles.

1·2. *n-vectors.*

Definition 1. An ordered set of n numbers is called an *n-vector*

$$\alpha = (a_1, a_2, \ldots, a_n).$$

The n numbers a defining α are called its *coordinates*. As the set is supposed to be an ordered one, the n-vector will in general be altered by the interchange of the coordinates.

Definition 2. The product of a number c and an n-vector α is the n-vector

$$c\alpha = (ca_1, ca_2, \ldots, ca_n).$$

Definition 3. The sum of α and an n-vector $\beta = (b_1, \ldots, b_n)$ is the n-vector

$$\alpha + \beta = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

From these definitions it follows:

$\alpha + \beta = \beta + \alpha$ *commutative law,*

$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ *associative law,*

$$c(\alpha + \beta) = c\ \alpha + c\ \beta \qquad \textit{1st distributive law,}$$

$$(c_1 + c_2)\alpha = c_1\ \alpha + c_2\ \alpha \qquad \textit{2nd distributive law.}$$

As these laws hold, one can use the notation of sum of n-vectors in the same manner as it is used for numbers. Thus

$$\Sigma c_j\ \alpha^j = (\Sigma c_j a^j{}_1, \ldots, \Sigma c_j a^j{}_n), \text{ where}$$

$j = 1, \ldots, m$; c_j are arbitrary numbers, and $\alpha = (a^j{}_1, \ldots, a^j{}_n)$ are n-vectors.

The n-vector $(-1)\alpha$ is called the *negative* of α, and is denoted by $-\alpha$. The inverse of the addition of α, is the addition of $-\alpha$. As in elementary arithmetic, this operation is called the *subtraction* of α, and is denoted by the sign $-$. Accordingly $\beta - \alpha$ is put for $\beta + (-\alpha)$.

Notations :

$0 = (0, 0, \ldots, 0)$	zero-vector
$\varepsilon^1 = (1, 0, \ldots, 0)$	first unit-vector
$\varepsilon^2 = (0, 1, \ldots, 0)$	second unit-vector
....	
$\varepsilon^n = (0, 0, \ldots, 1)$	n^{th} unit-vector.

Formulas : $\alpha - \alpha = 0$, $c\,0 = 0$, $\alpha = \Sigma a_j\ \varepsilon^j$.

The vectors of Plane Geometry can be considered as 2-vectors, those of Solid Geometry, as 3-vectors. In Geometry, these vectors are added by putting them together in such a manner that the endpoint of the first vector is the starting point of the second one. The result of the addition is the same as here ; n-vectors occur also on other occasions. Let e. g. n be the number of the depositers of a bank, and $a_1, a_2, \ldots, a_n$ be their balances at a certain day ; then the state of the bank on that day is represented by the n-vector $(a_1, a_2, \ldots, a_n) = \alpha$. Similarly the alteration of the state on that day is represented by an n-vector β, and the state of the bank on the following day is given by $\alpha + \beta$.

1·3. *Vectorspaces.*

Definition 1. An n-vector α is said to be *dependent* on the n-vectors α^j $(j = 1, \ldots, m)$ if α can be represented by $\alpha = \sum\limits_j c_j\ \alpha^j$.

Definition 2. The n-vectors depending on $\alpha^1, \ldots, \alpha^m$, are said to form a *vectorspace* generated by $\alpha^1, \ldots, \alpha^m$.

Proposition 1. If $\beta^1, \ldots, \beta^r$ belong to a vectorspace V, then every vector dependent on them belongs to V.

Proof. Let V be generated by $\alpha^1, \ldots, \alpha^m$, say $\beta^j = \sum_k b^j_k \alpha^k$, then $\sum_j c_j \beta^j = \sum_k d_k \alpha^k$, where $d_k = \sum_j c_j b^j_k$. Hence the proposition.

Definition 1 can also be expressed in this manner: α^{m+1} is dependent on $\alpha^1, \ldots, \alpha^m$, if there exists an equation

$$\Sigma k_j \alpha^j = 0, \text{ where } k_{m+1} \neq 0. \tag{1}$$

Definition 3. $\alpha^1, \ldots, \alpha^{m+1}$ are *independent*, if $\Sigma k_j \alpha^j = 0$ implies

$$k_1 = \ldots = k_{m+1} = 0.$$

From this definition and the above remark it follows directly:

Proposition 2. $m + 1 > 1$ n-vectors are independent, if and only if none of them is dependent on the m other ones; a single n-vector is "independent" if it is different from the zero-vector.

Definition 4. A set of independent n-vectors generating a vectorspace V, is called a *basis* of V.

Proposition 3. Every vectorspace V containing n-vectors $\neq 0$ has a basis.

Proof. Let V be generated by $\alpha^1, \ldots, \alpha^m$. If these n-vectors do not form a basis, then either they are all $=0$, or one of them, say α_m is dependent on the other ones. In the first case, V contains no n-vector $\neq 0$, in the second case, V is generated by $\alpha^1, \ldots, \alpha^{m+1}$. Thus one can reduce the number of the generating n-vectors, till one gets a generating system of independent n-vectors. At every step, the number of generating n-vectors decreases; hence after less than m steps the procedure cannot be repeated any more; i.e. the generating n-vectors are independent. Thus they form a basis.

Proposition 4. Let $\alpha^1, \ldots, \alpha^m$ be a basis of V, $\beta = \Sigma c_j \alpha^j$ and $c_m \neq 0$, then $\alpha^1, \ldots, \alpha^{m-1}, \beta$ is a basis of V.

Proof. Since β is contained in V, it follows from prop. 1, that every n-vector of the vectorspace V′ generated by $\alpha^1, \ldots, \alpha^{m-1}, \beta$ is contained in V; on the other hand α^m, and therefore every n-vector of V, belongs to V′. Hence V′ = V. To prove that the n-vectors are independent, we suppose that there exists a system of numbers $d_1, \ldots, d_{m-1}, d_m$ not all vanishing such that $0 = d_1 \ \alpha^1 + d_2 \ \alpha^2 + \dots + d_{m-1} \ \alpha^{m-1} + d_m \ \beta = (d_1 + d_m \ c_1) \ \alpha^1 + \dots + (d_{m-1} + d_m \ c_{m-1}) \ \alpha^{m-1} + d_m \ c_m \ \alpha^m$. Since $\alpha^1, \dots, \alpha^{m-1}$ are independent, $d_m \neq 0$, and furthermore $c_m \neq 0$ holds, the coefficients on the right hand side are not all vanishing; this contradicts to the supposition that $\alpha^1, \dots, \alpha^m$ are independent. Hence the proposition.

Proposition 5. Let V be a vectorspace, $\alpha^1, \dots, \alpha^m$ its basis, and $\beta^1, \dots, \beta^t$ be t independent n-vectors in V ; then we get a new basis of V on replacing t suitable elements of the basis by the n-vectors β^j ; thus $t < m$ holds.

Proof (By mathematical induction). From prop. 4 it follows that the theorem holds for $t=1$. Let it hold for $t=r$; without loss of generality, we suppose that $\beta^1, \dots, \beta^r, \alpha^{r+1}, \dots, \alpha^m$ is a basis of V. Thus $\beta^{r+1} = c_1 \beta^1 + \dots + c_r \ \beta^r + c_{r+1} \ \alpha^{r+1} + \dots + c_m \ \alpha^m$. As β^{r+1} is not dependent on $\beta^1, \dots, \beta^r$, at least one of the numbers $c_{r+1}, \dots, c_m$ is different from zero, say $c_{r+1} \neq 0$. From prop. 4 it follows that α^{r+1} can be replaced by β^{r+1} in the basis. Hence proposition 5.

Proposition 6. Every basis of a vectorspace V contains the same number of elements ; this number is called the *rank* of V.

Proof. Let m be the number of elements of a basis of V, and t be the number of elements of an arbitrary system of independent n-vectors in V. From prop.5 it follows that $t \leqq m$. Hence there exists one system of m, but no system of more than m independent n-vectors in V. The number of elements of any basis is therefore equal to the maximum number of independent n-vectors. Hence the proposition.

Definition 5. If every n-vector of a vectorspace V′ is an n-vector of V, then V′ is a *subspace* of V. This is denoted by

$$V' \subseteq V.$$

Proposition 7. If $V' \subseteq V$, either $V' = V$, or rank $V' <$ rank V.

Proof. The n-vectors $\beta^1, \dots, \beta^t$ which form a basis of V′ are t independent n-vectors of V. Thus it follows from prop.5 that t suitable n-vectors of any basis of V can be replaced by the β's. Hence V has a basis $\beta^1, \dots, \beta^t, \alpha^{t+1}, \dots, \alpha^m$, where $m =$ rank V. Hence $t \leqq m$. In the special case when $t = m$, the vectorspaces V and V′ have the same basis $\beta^1, \dots, \beta^t$, and this implies $V = V'$.

To state that the subspace V′ of V is different from V one uses the notation

$$V' \subset V.$$

Proposition 8. The rank of a vectorspace of n-vectors is at most n.

Proof. The n unit-vectors generate a vectorspace which contains every n-vector. Hence the proposition follows from prop. 7.

Proposition 9. Between $p > n$ of n-vectors there exists always a linear equation with coefficients not all vanishing.

Proof. If the proposition is not true, there must exist $p > n$ independent n-vectors, contrary to prop. 8.

Proposition 10. Let A be a system of n-vectors with the property that the sum of any two n-vectors of A as well as the product of any number and an n-vector of A belongs to A, then A is a vectorspace.

Proof. There cannot exist more than n independent n-vectors in A, say $\alpha^1, \ldots, \alpha^r$ are independent; then every n-vector of A depends on the α's, but every n-vector depending on them must belong to A; thus A is a vectorspace generated by $\alpha^1, \ldots, \alpha^r$.

Proposition 11. The n-vectors

$$\begin{aligned} \beta^1 &= (1, 0, \ldots, 0, b_1, \ldots, b_{n-r}) \\ \beta^2 &= (0, 1, \ldots, 0, c_1, \ldots, c_{n-r}) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \beta^r &= (0, 0, \ldots, 1, k_1, \ldots, k_{n-r}) \end{aligned} \tag{2}$$

are independent.

Proof. Suppose $\lambda = \Sigma d_j \beta^j$. Then $\lambda = (d_1, d_2, \ldots, d_r, q_1, \ldots, q_{n-r})$. Hence $\lambda \neq 0$, unless $d_1 = d_2 = \ldots = d_r = 0$.

1-4. *Matrices. The method of "Sweep out".*

Definition. A *matrix* M is a rectangular scheme consisting of nm numbers called the elements of M which are arranged in m (horizontal) *rows* and n (vertical) *columns*. The rows can be considered as n-vectors which generate a vectorspace R(M), and the columns are m-vectors generating a vectorspace C(M). If every element of M is equal to zero, M is called the *zero-matrix* 0.

Consider e.g. the right hand side of 1-3, (2). Here $m = r$. The row-vectors are independent, hence rank R(M) $= r$; the first r column-vectors are also independent, and since the vectors are m-vectors, rank C(M) $= r$. It will be proved that the ranks of those two vectorspaces are always equal, and this number will be called the rank of the matrix M. To get this result, some operations will be introduced which neither alter the vectorspace R(M), nor the rank of the vectorspace C(M). By these operations the matrix is gradually "*swept out*", *i.e.* in a certain portion of the matrix, the elements are replaced by zero, and finally the matrix is reduced to a type which is similar to the matrix 1-3, (2). The method of "sweep out" is very important for the solution of systems of linear equations. Let A be the matrix

$$\mathrm{A} = (\,(a^i{}_k)\,) = \begin{pmatrix} a^1{}_1, \ldots, a^1{}_n \\ \cdots\cdots\cdots\cdots \\ a^m{}_1, \ldots, a^m{}_n \end{pmatrix}. \tag{1}$$

and let $\alpha^1, \ldots, \alpha^m$ be the n-vectors formed by the rows. The vectorspace R(A) is obviously not altered by the following operations :

I Replace α^j by $c\alpha^j$, where $c \neq 0$ (row-multiplication).
II Replace α^j by $\alpha^j + d\alpha^k$ (row-addition).
III Omit α^k, if $\alpha^k = 0$. (row-omission).

Let $\alpha_1, \ldots, \alpha_n$ be the m-vectors formed by the columns, and let

$$\Sigma g_s \, \alpha_s = 0 \tag{2}$$

hold. It will be shown that the same equation holds after any one of the operations I, II, III, has been performed on the matrix A. Of course (2) can be expressed by

$$\Sigma g_s \, a^i{}_s = 0, \tag{2'}$$

for $i = 1, \ldots, m$.

Then for any particular j, k the equations $\Sigma g_s \, c a^j{}_s = 0$

$$\text{and} \qquad \Sigma g_s \, (a^j{}_s + d a^k{}_s) = 0$$

hold ; hence (2′) remains invariant for the operations I and II. The operation III means only the omission of a condition which is identically satisfied. Hence every linear equation (2) between the column-vectors is invariant for the operations I, II, III. The inverse operation of I is an operation of the same type where c is replaced by c^{-1} ; the inverse operation of II is an operation II where d is replaced by $-d$; the inverse operation of III is the addition of a new coordinate which takes the value 0 for every column-vector. Hence, a linear equation (2) cannot hold after the operation I, II, III unless it held before. Let r of the column-vectors be independent, and the other column-vectors be dependent on them, then these r vectors form a basis, and rank $C(A) = r$. By the operations I, II, III, those r vectors remain independent and the other vectors are dependent on them. Hence the rank of $C(A)$ is not altered. The essence of these considerations can be formulated in the following manner.

Proposition 1. By repeated use of the operations I, II, III the vectorspace $R(A)$ and the rank of the vectorspace $C(A)$ are not altered.

It may be noticed that the vectorspace $C(A)$ will in general be altered, e.g. the number of the coordinates may decrease; on the other hand rank $R(A)$ is invariant, since $R(A)$ itself is not altered.

Theorem 1. By repeated use of the operations I, II, III, the matrix $A \neq 0$ can be transformed into

$$\begin{pmatrix} 1, 0, \ldots, 0 & *, \ldots, * \\ 0, 1, \ldots, 0 & *, \ldots, * \\ \cdots\cdots\cdots & \cdots\cdots \\ 0, 0, \ldots, 1 & *, \ldots, * \end{pmatrix} \tag{3}$$

or into a matrix which differs from (3) by a permutation of the columns only. (Asterisks are put for numbers of any value). The rows of this matrix form a basis of $R(A)$.

Proof. If any row-vector is equal to 0, this row should be omitted. Neither by I nor by II, the matrix can be transformed into 0. Thus we will suppose that at every later stage of the operations given in this proof, every row-vector 0 will be omitted automatically; the matrix cannot be annihilated thereby. Let a^1_1 be different from zero, replace α^1 by $(a^1_1)^{-1}\,\alpha^1$, thus a^1_1 is made equal to 1 by the operation I; then replace α^i by $\alpha^i - a^i_1\,\alpha^1$ (operation II) for $i = 2, 3, \ldots, m$. By this sequence of operations, the first column is "swept out"; i.e. one element (the first one) is made one, whereas the other elements are made zero; by the following operations the first row will not be multiplied by any number, and it will not be added to any other row; hence the first column will remain "swept out". If $a^1_1 = 0$, there exists a number j_1, so that $a^1_{j_1} \neq 0$; then we consider the column j_1 as the "first" column and we sweep it out accordingly. Since in the proposition of the theorem a permutation of the columns does not matter, we may suppose without loss of generality that $j_1 = 1$. After the first column is swept out, we denote the elements again as in (1). Now $a^2_1 = 0$, and every row with vanishing elements is omitted; hence there is an element $a^2_{j_2} \neq 0$, for which $j_2 > 1$. Without loss of generality we can suppose $j_2 = 2$. Again we sweep out the second column on replacing α^2 by $(a^2_2)^{-1} \alpha^2$ and α^k by $\alpha^k - a^k_2 \alpha^2$ for $k \neq 2$. In this manner we can repeat the procedure till the matrix is either reduced to the form (3), or differs from it by a permutation of the columns only. The rows of the matrix generate R(A) and as they are independent (see 1-3, prop.11), they form a basis of R(A).

Theorem 2. rank R(A)=rank C(A) for every matrix A. This number is called the *rank of the matrix A*.

Proof. If A is the zero-matrix, then both the vectorspaces are of rank zero. If $A \neq 0$, then we sweep out A ; by these operations the ranks are not altered as shown by prop. 1. In (3), the rank of both the vectorspaces is equal to the number of rows ; the same holds for the matrices which one gets by interchanging the columns of (3). Hence the theorem.

1-5. *Orthogonality. Homogeneous linear equations.*

Definition. Two n-vectors $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$ are said to be *orthogonal* if

$$\sum_i a_i\, b_i = 0 \text{ holds.}$$

Thus if α is orthogonal to β, then β is orthogonal to α ; *i.e.* orthogonality is a *symmetric* relation. This notation offers the opportunity to apply vectors to systems of linear equations. Consider at first *homogeneous* equations.

$$\begin{array}{c} a^1{}_1\, x_1 + \ldots + a^1{}_n\, x_n = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a^m{}_1\, x_1 + \ldots + a^m{}_n\, x_n = 0. \end{array} \tag{1}$$

For the matrix $((a^i{}_k))$ its rows etc. we use the notations of 1-4. Every ordered system of numbers

$$\xi = (x_1, \ldots, x_n) \tag{2}$$

which satisfies the equations (1) is called a *solution* of (1). *A solution is therefore an n-vector which is orthogonal to* $\alpha^1, \ldots, \alpha^m$. Let (2) be a solution of (1) and let $\sum_j c_j\, \alpha^j{}_n = (a_1, \ldots, a_n)$ be an arbitrary vector of the vectorspace R(A). As

$$\sum a^j{}_i\, x_i = 0$$

holds for $j = 1, \ldots, m$,

BCU 1741

$$0 = \sum_j c_j \sum_i a^j_i\, x_i = \sum_i x_i \sum_j c_j\, a^j_i = \sum_i x_i\, a_i.$$

Hence ξ is orthogonal to α. I.e.

Proposition 1. Every solution of (1) is orthogonal to every vector of R(A).

If ξ is a solution of (1) and c is any number, then $c\xi$ is also a solution of (1).

Let furthermore

$$\eta = (y_1, \ldots, y_n) \tag{2'}$$

be a solution of (1), then for $j = 1, \ldots, m$,

$$0 = \sum a^j_i\, x_i + \sum a^j_i\, y_i = \sum a^j_i\, (x_i + y_i)$$

holds. Hence $\xi + \eta$ is also a solution of (1).

From 1-3 prop.10 it follows that the solutions of (1) form a *vectorspace*. Every n-vector of this vectorspace is orthogonal to every n-vector of R(A). Hence :

Proposition 2. The solutions of (1) form a vectorspace X(A). Every n-vector of X(A) is orthogonal to every n-vector of R(A).

To get the solutions of (1), one need only know the vectors which are orthogonal to any basis of R(A). Using the method of sweep out, one gets the basis in a suitable standard form

$$\begin{pmatrix} 1, 0, \ldots, 0, & -b^1_1, \ldots, & -b^1_{n-r} \\ 0, 1, \ldots, 0, & -b^2_1, \ldots, & -b^2_{n-r} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ 0, 0, \ldots, 1, & -b^r_1, \ldots, & -b^r_{n-r} \end{pmatrix} \tag{3}$$

(the asterisks of 1-4, (3) have been replaced by $-b^i_k$) or by a matrix, which differs from (3) by a suitable permutation of the columns. Let

$$\begin{pmatrix} 1, & \ldots, & n \\ i_1, & \ldots, & i_n \end{pmatrix} \tag{4}$$

be this permutation. An n-vector (2) is orthogonal to the n-vectors of R(A) and is therefore a solution of (1) if and only if it satisfies the conditions

$$x_{i_j} = b^j_1\, x_{i_{r+1}} + \ldots + b^j_{n-r}\, x_{i_n}, \text{ for } j = 1, \ldots, r. \tag{5}$$

The values of $x_{i_{r+1}}, \ldots, x_{i_n}$ can be chosen arbitrarily, the remaining r coordinates of the n-vector are uniquely defined by them.

Gs 3578

Put e.g. $x_{i_{r+1}}, \dots, x_{i_n} = (1, 0, \dots, 0)$,

then $x_{i_1}, \dots, x_{i_r} = (b^1{}_1, b^2{}_1, \dots, b^r{}_n)$.

Thus one gets $n - r$ independent n-vectors of X(A) which have the coordinates, ordered corresponding to the permutation (4). Hence$(x_{i_1}, \dots, x_{i_n})$ take the following sets of values,

$$\begin{array}{l} (b^1{}_1, \dots, b^r{}_1, \ 1, 0, \dots, 0) \\ (b^1{}_2, \dots, b^r{}_2, \ 0, 1, \dots, 0) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ (b^1{}_{n-r}, \dots, b^r{}_{n-r}, 0, 0, \dots, 1). \end{array} \tag{6}$$

These n-vectors form the basis of a vectorspace X′ of rank $(n - r)$, and X′ is a subspace of X(A). In X′, the coordinates $x_{i_{r+1}}, \dots, x_{i_n}$ take every set of values, but from (5) it follows that by these values a solution of (1) is uniquely determined. Hence every solution of (1) is an n-vector of X′, hence X′ = X(A). This result will be formulated by the following propositions :

Proposition 3. rank R(A) + rank X(A) = n. (7)

Proposition 4. To solve (1), one applies the method of "sweep out" to the matrix A ; let the result be a matrix, which differs from (3) by a permutation (4) of the columns only ; then a basis of X(A) is given by (6).

Every n-vector α of R(A) is orthogonal to every n-vector of X(A). The n-vectors which are orthogonal to the n-vectors of X(A) form a vectorspace of rank $n - (n - r) = r$ which contains R(A) as a subspace. From 1-3, prop. 7 it follows that this vectorspace is identical with R(A). This result can be expressed by :

Proposition 5. If $\Sigma\, a_i\, x_i = 0$ is satisfied by every solution of (1), then $(a_1, \dots, a_n)$ is an n-vector of R(A).

The propositions 1, 2, 3, 5 can be condensed into the following theorem.

Theorem. Every system (1) of homogeneous linear equations generates two vectorspaces R(A) and X(A) for which (7) holds. R(A) is generated by the rows of (1) ; X(A) consists of the solutions of (1). An n-vector is orthogonal to R(A) [to X(A)] if and only if it belongs to X(A) [to R(A)].

It is important for the theory of homogeneous linear equations and its applications that the problem of solving such equations leads to two vectorspaces which are connected by a reciprocity or duality. R(A) defines X(A) in the same manner as X(A) defines R(A).

The advantage of the use of homogeneous systems is mainly based on this fact. The treatment of non-homogeneous systems is more complicated. One may apply to them the method of homogeneisation as it will be done in the following article. This method is used also in geometry, when ordinary coordinates are replaced by homogeneous ones, and thereby the space is extended to a projetive space. The duality so obtained corresponds exactly to the duality between X(A) and R(A).

1·6. *Systems of non-homogeneous linear equations.*
Given a system of linear equations

$$\begin{aligned} a^1{}_1\, x_1 + \dots + a^1{}_n\, x_n &= a^1{}_0 \\ \dots\dots\dots\dots\dots\dots & \\ a^m{}_1\, x_1 + \dots + a^m{}_n\, x_n &= a^m{}_0. \end{aligned} \qquad (1).$$

If the terms on the righthand side are not all equal to zero, the system will be considered jointly with the following two homogeneous systems :

$$\begin{aligned} a^1{}_1\, y_1 + \dots + a^1{}_n\, y_n &= 0 \\ \dots\dots\dots\dots\dots\dots & \\ a^m{}_1\, y_1 + \dots + a^m{}_n\, y_n &= 0, \end{aligned} \qquad (2)$$

and

$$\begin{aligned} a^1{}_1\, z_1 + \dots + a^1{}_n\, z_n - a^1{}_0\, z_0 &= 0 \\ \dots\dots\dots\dots\dots\dots & \\ a^m{}_1\, z_1 + \dots + a^m{}_n\, z_n - a^m{}_0\, z_0 &= 0. \end{aligned} \qquad (3)$$

The matrix of (2) is denoted by A, and the matrix of (3) by A_0. The following propositions are obvious, though important :

Proposition 1. If $\xi = (x_1, \dots, x_n)$ is a solution of (1), and $\eta = (y_1, \dots, y_n)$ is a solution of (2), then $\xi + \eta$ is a solution of (1).

Proposition 2. If ξ and ξ^1 are solutions of (1), then $\eta = \xi - \xi^1$ is a solution of (2).

Proposition 3. If $\xi^1, \dots, \xi^s$ are solutions of (1), and $c_1 + \dots + c_s = 1$, then $\xi = c_1\, \xi^1 + \dots + c_s\, \xi^s$ is a solution of (1).

Proposition 4. If $(x_1, \dots, x_n)$ is a solution of (1), then $(x_1, \dots, x_n, 1)$ is a solution of (3).

Proposition 5. Let $(z_1, \dots, z_n, z_0)$ be a solution of (3). If $z_0 = 0$, then $(z_1, \dots, z_n)$ is a solution of (2) : if $z_0 \neq 0$, then $(z_1 : z_0, \dots, z_n : z_0)$ is a solution of (1).

The propositons 1 and 2 can be condensed into the following theorem.

Theorem 1. If ξ is an arbitrary solution of (1), then we get all the solutions of (1) by adding to ξ the solutions η of (2).

As has been shown in the introduction, (1) may have no solution. A necessary and sufficient condition for the existence of solution will now be established.

Theorem 2. The system (1) has solutions if and only if rank A $=$ rank A_0.

Proof. Let r be the rank of A. Since r is equal to the rank of the vectorspace generated by the columns of A, and A_0 is formed by A and a column added to A, rank A_0 is either equal to r or to $r + 1$. The solutions of (2) form a vectorspace X(A) of rank $n - r$. Let

$$(y_1, \dots, y_n) \tag{4}$$

be the vectors of this space. The vectors

$$(y_1, \dots, y_n, 0) \tag{5}$$

form a vectorspace X′ consisting of $(n + 1)$-vectors. n-vectors (4) are independent if and only if the corresponding vectors (5) are independent. Hence

$$\text{rank } X' = \text{rank } X(A) = n - r.$$

Also $X' \subseteq X(A_0)$, since every vector of X′ is a solution of (3). Hence

$$n - r = \text{rank } X' \leq \text{rank } X(A_0) = (n + 1) - \text{rank } A_0, \tag{6}$$

where equality holds if and only if the vectorspaces X′ and $X(A_0)$ are identical. But X′ is identical with $X(A_0)$ if in every solution of (3) the coordinate z_0 is equal to zero; from prop. 5 it follows that in this case (1) has no solution. Hence for $n - r = n + 1 - \text{rank } A_0$, that is, when rank $A_0 = r + 1$, the system (1) has no solution. If $X(A_0)$ contains $(n + 1)$-vectors not belonging to X′, then it follows from prop. 5 that (1) has solutions. This holds if and only if $n - r < n + 1 - \text{rank } A_0$, *i. e.* rank $A < r + 1$. Therefore in this case rank $A_0 = r$. Hence theorem 2.

To find out the solutions of (1), one may solve the homogeneous system (3) by the method of sweep-out and consider those solutions only for which $z_0 = 1$ holds. The method of sweep-out leads to a matrix with $n + 1$ columns and $t = \text{rank } A_0$ rows [see 1-5, (3)] of the type

$$\begin{pmatrix} 1, 0, \ldots, 0, -b^1_1, \ldots, -b^1_{n+1-t} \\ 0, 1, \ldots, 0, -b^2_1, \ldots, -b^2_{n+1-t} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0, 0, \ldots, 1, -b^t_1, \ldots, -b^t_{n+1-t} \end{pmatrix}.$$

This matrix corresponds to a system of homogeneous linear equations which is equivalent to (3):

$$\begin{aligned} z_{i_1} &= b^1_1\, z_{i_{t+1}} + \ldots + b^1_{n+1-t}\, z_{i_{n+1}} \\ z_{i_2} &= b^2_1\, z_{i_{t+1}} + \ldots + b'_{n+1-t}\, z_{i_{n+1}} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ z_{i_t} &= b^t_1\, z_{i_{t+1}} + \ldots + b^t_{n+1-t}\, z_{i_{n+1}}, \end{aligned}$$

where $i_1, \ldots, i_n, i_{n+1}$ is a permutation of the indices $1, \ldots, n, 0$. If none of the indices $i_1, \ldots, i_t$ is the index 0, then we can suppose without loss of generality that i_{n+1-t} is zero. Then the system (1) is equivalent to

$$\begin{aligned} x_{i_1} &= b^1_1\, x_{i_{t+1}} + \ldots + b^1_{n-t}\, x_{i_n} + b^1_{n+1-t} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_{i_t} &= b^t_1\, x_{i_{t+1}} + \ldots + b^t_{n-t}\, x_{i_n} + b^t_{n+1-t}. \end{aligned} \tag{7}$$

In this case, the equations are solvable, and therefore $r = t$ holds. The case of insolvability can therefore occur only if we cannot sweep out the matrix A_0 without sweeping out the last column of it, i.e. if there comes out a row in which every element except the last one is zero. A row of this kind corresponds to the condition $z_0 = 0$, and if this condition is satisfied, the system (1) has no solution. Hence:

Theorem 3. On applying the method of sweep out to the matrix A_0 in such a manner that the coefficients of z_0 remain the last column, either one gets a solution (7) or a row comes out which corresponds to an equation $z_0 = 0$, and which shows that the system (1) has no solution.

From 1·5 and 1·6 it follows that the solvability of a system of linear equations does not depend on the number of the equations and of the unknown quantities, but on the ranks of certain matrices. These ranks are limited by the number of the equations and of the unknown quantities as the rank of a matrix can neither exceed the number of the rows, nor the number of the columns.

Proposition 6. If $m = n$, the system (1) has exactly one solution if and only if rank $A = n$.

Proof. Rank $A = n'$ cannot exceed n. If $n' < n$, then either (1) has no solution or its solutions are in a (1, 1)-correspondence to the solutions of (2) [see theorem 1] and the solutions of (2) form a vectorspace of rank $n - n'$ [see 1-5, prop. 2 and 3], and this vectorspace contains more than one element. If rank $A = n$, then the solutions of (2) form a vectorspace of rank 0, i.e. the system (2) has the trivial solution $(0, \ldots, 0)$ only. As rank A_0 cannot exceed n, rank A_0 = rank A ; there exists therefore a solution of (1), but from theorem 1 it follows that there exists one solution only.

The coordinates of n-vectors and the elements of matrices have been supposed to be "numbers". No special supposition has been made whether this term should be understood as *real* numbers or as *complex* numbers. Of course the preceding investigations are made in such a manner, that they are independent of any special supposition. It may be mentioned in anticipation that the investigations up to here hold unaltered if the notion of number is replaced by the notion of "element of any particular[*] field". The general notion of field will be explained in Chapter II, and will not be used before.

1-7. *The method of orthogonalisation.*[†]

The numbers occuring in this section are supposed to be real.[‡] Especially the n-vectors are supposed to have real coordinates.

Definition 1. The *scalar product* of two n-vectors $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$ is the number

$$\alpha\,\beta = \sum_i a_i\, b_i .$$

From this definition follow :

1. $\alpha\beta = \beta\alpha$ *commutative law.*
2. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ *distributive law.*
3. $\alpha\beta = 0$, if and only if α is orthogonal to β.
4. $\alpha\alpha > 0$, if $\alpha \neq 0$
   $= 0$, if $\alpha = 0$.

---

[*] The field may also be finite ; in this case a vectorspace contains a finite number of elements only. That vectorspaces are infinite sets of vectors, has not been used anywhere (see especially the Proof of 1-6, prop. 6).

[†] This section may be omitted at a first reading.

[‡] The method can easily be generalised for *abstract real fields* i. e. fields in which 0 cannot be represented as a sum of squares.

Definition 2. The non-negative square root of $\alpha\alpha$ is said to be the *length* $|\alpha|$ of α.

Thus $|\alpha| > 0$, unless $\alpha = 0$. That the length is a generalisation of the notion of absolute value, is seen from the case $n = 1$, and also from the case $n = 2$, when $\alpha = (a_1, a_2)$ is represented by the complex number $a_1 + a_2 i$. This justifies the notation $|\alpha|$. Given a system of homogeneous linear equations with the matrix A. To solve the system by the method of orthogonalisation, one forms a system of n independent n-vectors of length 1

$$\beta^1, \dots, \beta^r, \beta^{r+1}, \dots, \beta^n, \tag{1}$$

each of them being orthogonal to each other in such a way, that

$$\beta^1, \dots, \beta^r \tag{2}$$

is a basis of the vectorspace R(A) generated by the rows of A. The vectorspace generated by

$$\beta^{r+1}, \dots, \beta^n \tag{3}$$

contains only n-vectors which are orthogonal to the n-vectors of R(A), and these are solutions of the given system. It will be shown how the n-vectors (1) can be found, and that (3) is a basis of X(A). By these considerations, one gets a second proof of 1·5, prop.3.

Definition 3. The n-vectors $\beta^1, \dots, \beta^m$ form an *orthogonal system*, if

$$\begin{aligned} \beta^i \beta^k &= 0, \qquad \text{for } i \neq k \\ &= 1, \qquad \text{for } i = k. \end{aligned} \tag{4}$$

The n-vectors of an orthogonal system are therefore of length 1, and are mutually orthogonal.

Let

$$\beta^1, \beta^2, \dots, \beta^m \tag{5}$$

be an orthogonal system, and

$$\alpha = \Sigma\, c_i\, \beta^i, \tag{6}$$

then it follows that

$$\alpha\, \beta^k = c_k, \text{ for } k = 1, \dots, m. \tag{7}$$

Hence $\alpha = 0$ implies $c_1 = \dots = c_m = 0$. Thus:

Proposition 1. The n-vectors of an orthogonal system are independent.

Let κ be an arbitrary n-vector; put in (6):

$$c_i = \kappa\beta^i, \text{ and } \lambda = \kappa - \alpha, \tag{8}$$

then it follows from (7) that

$$\lambda\, \beta^k = 0, \text{ for } k = 1, \ldots, m.$$

λ is therefore orthogonal to the n-vectors (5). If $\lambda \neq 0$, then put

$$|\, \lambda\, |^{-1}\, \lambda = \beta^{m+1}, \tag{9}$$

then the n-vectors

$$\beta^1, \ldots, \beta^{m+1} \tag{10}$$

form an orthogonal system. As β^{m+1} is independent of the n-vectors (5), so are λ, and κ. If $\lambda = 0$, then $\kappa = \alpha$ is dependent on (5). Hence

Proposition 2. If κ is independent of (5), and β^{m+1} is defined by (6), (8) and (9), then (10) is an orthogonal system, and the vectorspace generated by (10) is the same as the vectorspace generated by $\beta^1, \ldots, \beta^m, \kappa$. If $\lambda = 0$, then κ is dependent on (5).

Proposition 2 can be applied for two different purposes. Firstly: To extend an orthogonal system (5) to an orthogonal system (10) in such a manner that a particular n-vector κ which is independent of (5) is dependent on (10). Secondly: To state whether an arbitrary n-vector is dependent on (5).

Let

$$\begin{matrix} \beta^1 = (b^1{}_1, \ldots, b^1{}_n) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \beta^m = (b^m{}_1, \ldots, b^m{}_n) \end{matrix} \tag{11}$$

be an orthogonal system; to find out if the unit-vector ϵ^k is dependent on (5), put in (8) $\kappa = \epsilon^k$, and therefore $c_i = \epsilon^k \beta^i = b^i{}_k$; hence

$$\alpha = \sum_i b^i{}_k\, \beta^i = (\sum_i b^i{}_k\, b^i{}_1, \ldots, \sum_i b^i{}_k\, b^i{}_n).$$

Hence $\lambda = 0$ if and only if

$$\sum_i b^i{}_k\, b^i{}_j = 1, \text{ for } k = j$$
$$= 0, \text{ for } k \neq j.$$

Hence ϵ^k is dependent on (5) if and only if the *column-vector* β_k of (11) is of length 1 and orthogonal to other column-vectors of (11). For $m < n$, one finds easily by this method a unit-vector which is independent of (5).

To-apply the method of orthogonalisation to a matrix A, omit the row-vectors which are equal to 0.

Put $$|\alpha^1|^{-1}\,\alpha^1 = \beta^1,$$

omit the rows of A dependent on β^1,

put $$\lambda = \alpha^2 - (\alpha^2\,\beta^1)\,\beta^1, \quad \beta^2 = |\lambda|^{-1};$$

omit the rows of A dependent on β^1, β^2,

put $$\lambda' = \alpha^3 - [(\alpha^3\,\beta^1)\;\beta^1 + (\alpha^3\,\beta^2)\;\beta^2],\; \beta^3 = |\,\lambda'\,|^{-1}\,\lambda'$$

and continue till one gets the orthogonal system (2) of independent n-vectors which forms a basis of R(A).

This orthogonal system can furtheron be extended by the help of an n-vector κ which is independent of it. One may choose this vector e.g. out of the unit-vectors. The procedure can be repeated and stops after n steps as the n orthogonal n-vectors

$$\beta^1, \ldots, \beta^r, \beta^{r+1}, \ldots, \beta^n$$

are independent and form therefore a basis of the complete vectorspace of rank n.

An arbitrary n-vector can be represented by

$$\alpha = \Sigma\, c_i\, \beta^i, \text{ where } \alpha\,\beta^k = c_k, \text{ for } k = 1, \ldots, n.$$

α is a solution to the system of homogeneous equations with the matrix A if and only if it is orthogonal to R(A), *i. e.* if it is orthogonal to $\beta^1, \ldots, \beta^r$. Hence α is a solution if and only if

$$c_1 = \ldots = c_r = 0;$$

hence the solutions are the n-vectors dependent on

$$\beta^{r+1}, \ldots, \beta^n.$$

By this result 1-5 prop.3 is proved without reference to the method of sweep out.

The method of orthogonalisation has some advantage over the method of sweep out, as it furnishes bases of the vectorspaces R(A) and X(A) which are orthogonal systems, but it is not very convenient for practical calculation. "Sweep out" needs only rational operations whereas for orthogonalisation, a square root must be drawn at every step.

1·8. *Determinants.*

Let $A = ((a^i_k))$ be a square shaped matrix with n rows and n columns. It is possible to allot to A a certain number which therefore is a *function* of the matrix. One may consider this value also as a function of the n^2 elements of the matrix or as a function of the n column-vectors; for when the elements or the column-vectors are given in their proper order, the matrix is given too. Obviously functions of n^2 variables can be formed in an infinity of different ways. The particular function which will be considered here, is called a *determinant*, and it is denoted by

$$\det \mathrm{A} = \det ((a^i_k)) = \begin{vmatrix} a^1_1, & \ldots, & a^1_n \\ \ldots & \ldots & \ldots \\ a^n_1, & \ldots, & a^n_n \end{vmatrix} = \det (\alpha_1, \ldots, \alpha_n). \tag{1}$$

One may consider $\alpha_1, \ldots, \alpha_n$ as an abbreviation put for the vertical column-vectors of $((a^i_k))$; then the notation given on the right hand side becomes identical with the notation on the left. It is however useful to express the determinant as a function of the column-vectors, since the determinant will be shown to be a linear function of those n-vectors.

The determinant is supposed to have the following properties :

(*a*) $\det (\alpha_1, \ldots, c\,\alpha_m, \ldots, \alpha_n) = c \det (\alpha_1, \ldots, \alpha_n)$.

(*b*) $\det (\alpha_1, \ldots, \alpha_m + \alpha_k, \ldots, \alpha_n) = \det (\alpha_1, \ldots, \alpha_n)$, for $k \neq m$.

(*c*) $\det (\varepsilon^1, \ldots, \varepsilon^n) = 1$.

It is not obvious that there exists a function which has these properties. It may be that these contradict one another. If e.g. in (*b*) the restriction $k \neq m$ is omitted, the conditions contradict one another, since from (*a*) and (*c*) it follows that $\det (2\varepsilon^1, \ldots, \varepsilon^n) = 2$, whereas from (*b*) and (*c*) it would follow that it is equal to 1. We *assume* at first that such a function exists and derive its properties ; existence and uniqueness will be proved later on.

Proposition 1. If anyone of the n-vectors $\alpha_1, \ldots, \alpha_n$ is equal to 0, then det A is zero.

Proof. Let $\alpha_i = 0$, and therefore $\alpha_i = 0\,\alpha_i$,

$$\det \mathrm{A} = \det (\alpha_1, \ldots, 0\,\alpha_i, \ldots, \alpha_n) = 0 \det \mathrm{A} = 0.$$

Proposition 2. det A is not altered when α_k is replaced by $\alpha_k + c\alpha_i$, for $i \neq k$.

Proof. For $c = 0$, the proposition is obvious, for $c \neq 0$, det A $= \dfrac{1}{c} \det (\ldots, c\alpha_i, \ldots, \alpha_k, \ldots) = \dfrac{1}{c} \det (\ldots, c\alpha_i, \ldots, \alpha_k + c\alpha_i, \ldots) =$ $\det (\ldots, \alpha_i, \ldots, \alpha_k + c\,\alpha_i, \ldots)$.

This proposition shows that "column-additions" do not alter a determinant where column-addition is understood in the same sense as "row-addition" was in 1·4 If any column is dependent on the other columns, say $\alpha_n = c_1 \alpha_1 + \dots + c_{n-1} \alpha_{n-1}$, one can reduce it by $n - 1$ column-additions to the n-vector 0. From prop. 1, it follows therefore :

Proposition 3. When the column-vectors are dependent, the determinant is equal to zero.

Another consequence of prop. 2 is :

Proposition 4. If two columns are interchanged, the determinant changes its sign.

Proof.
$$\begin{aligned} \det \mathrm{A} &= \det (\dots, \alpha_i, \dots, \alpha_k, \dots) \\ &= \det (\dots, \alpha_i, \dots, \alpha_k + \alpha_i, \dots) \\ &= \det (\dots, \alpha_i - (\alpha_k + \alpha_i), \dots, \alpha_k + \alpha_i, \dots) \\ &= \det (\dots, - \alpha_k, \dots, \alpha_i, \dots) \\ &= - \det (\dots, \alpha_k, \dots, \alpha_i, \dots). \end{aligned}$$

From this proposition follows :

Proposition 5. An even permutation of the columns does not alter a determinant ; an odd permutation alters a determinant to its negative.

Proposition 6. $\det (\varepsilon^{i_1}, \dots, \varepsilon^{i_n}) = +1$, or $= -1$ according as the permutation $i_1, \dots, i_n$ is even or odd.

A determinant with two equal columns is equal to zero ; this is a special case of prop. 3. (it is also a consequence of prop. 4).

Proposition 7. Let B be the matrix which one gets by replacing a particular column α_i of A by β, then
$$\det \mathrm{A} + \det \mathrm{B} = \det (\alpha_1, \dots, \alpha_i + \beta, \dots, \alpha_n). \tag{2}$$

Proof. Let the $n - 1$ column-vectors α_k (for $k \neq i$) be dependent, then the three determinants occuring in (2) are zero each and the formula holds. Let α_i depend on the $n-1$ n-vectors α_k, then $\det \mathrm{A} = 0$, and the determinant on the right hand side of (2) can be reduced by column-addition to det B. Without loss of generality, we can therefore suppose, that $\alpha_1, \dots, \alpha_n$ are independent ; they therefore form a basis of the vectorspace containing every n-vector ; hence β depends on them, say $\beta = c_1 \alpha_1 + \dots + c_n \alpha_n$. By column-addition, it is possible to reduce the column β in B to $c_i \alpha_i$, and similarly in the determinant on the right hand side of (2). Hence both the sides are equal to $(1 + c_i)$ det A. Hence the proposition.

Let B_ν be the matrix one gets by replacing α_i by β_ν, and let

$$\alpha_i = c_1 \beta_1 + \dots + c_i \beta_i ;$$

then

$$\det A = \det (\alpha_1, \dots, \sum_1^{i-1} c_\nu \beta_\nu, \dots, \alpha_n) + \det (\alpha_1, \dots, c_i \beta_i, \dots, \alpha_n)$$

$$= \det (\alpha_1, \dots, \sum_1^{i-1} c_\nu \beta_\nu, \dots, \alpha_n) + c_i \det B_i .$$

By repetition of this procedure one gets

$$\det A = c_1 \det B_1 + \dots + c_i \det B_i . \tag{3}$$

This formula can be expressed as follows:

Proposition 8. A determinant is a linear function of each of its column-vectors.

Consider especially $\alpha_i = (a^1{}_i, a^2{}_i, \dots, a^n{}_i) = \sum_k a^k{}_i \, \varepsilon^k$ and let

$$A^k{}_i = \det (\alpha_1, \dots, \alpha_{i-1}, \varepsilon^k, \alpha_{i+1} \dots, \alpha_n) ; \tag{4}$$

then we get from prop. 8:

Proposition 9. $$\det A = \sum_k a^k{}_i \, A^k{}_i . \tag{5}$$

The number $A^k{}_i$ is said to be the *cofactor* of $a^k{}_i$. If A_i is the n-vector $A_i = (A^1{}_i, \dots, A^n{}_i)$, then det A is the scalar product

$$\det A = \sum \alpha_i \, A_i .$$

Especially $$A^k{}_1 = \det (\varepsilon^k, \alpha_2, \dots, \alpha_n)$$

and $$\det A = \sum_k a^k{}_1 \det (\varepsilon^k, \alpha_2, \dots, \alpha_n).$$

By applying prop. 9 to $A^k{}_1$, one gets

$$A^k{}_1 = \sum_s a^s{}_2 \det (\varepsilon^k, \varepsilon^s, \alpha_3, \dots, \alpha_n), \text{ and therefore}$$

$$\det A = \sum_{k, s} a^k{}_1 \, a^s{}_2 \det (\varepsilon^k, \varepsilon^s, \alpha_3, \dots, \alpha_n).$$

By repeating this procedure n-times one gets:

$$\det A = \sum_{k, s, \dots, q} a^k{}_1 \, a^s{}_2, \dots, a^q{}_n \det (\varepsilon^k, \varepsilon^s, \dots, \varepsilon^q), \tag{6}$$

where $k, s, \ldots, q$ take the values $1, \ldots, n$ independently. The determinants on the right hand side take the values $+1$, -1, 0 according as $k, s, \ldots, q$ is an even permutation of $1, \ldots, n$, or an odd permutation of them, or the indices are not different. Hence :

Proposition 10. If there exists a function det A satisfying the conditions (*a*), (*b*), (*c*), then det A must be equal to.

$$D(A) = \Sigma \pm a^k{}_1, \ldots, a^q{}_n, \tag{7}$$

where the sum has to be taken over all those products $a^k{}_1 \ldots a^q{}_n$ for which the upper indices are permutations of $1, \ldots, n$; the sign $+$ being used for even, $-$ for odd permutations.

Theorem 1. The function det A satisfying the conditions (*a*), (*b*), (*c*), exists and it is equal to the function D(A) as defined by (7).

Proof. From prop.10 it follows that det A is either non-existant or it is equal to D(A). To prove the theorem, it must therefore be shown that D(A) satisfies the conditions (*a*), (*b*), (*c*). Thus : (*a*) If α_i is replaced by $c\alpha_i$, then in every term of the sum (7) exactly one factor is multiplied by c ; hence D(A) is replaced by cD(A). (*c*) If $\alpha_j = \epsilon^j$ for $j = 1, \ldots, n$, then $a^j{}_j = 1$, $a^j{}_k = 0$ for $j \neq k$. Hence $a^1{}_1\, a^2{}_2, \ldots, a^n{}_n = 1$, whereas the other terms in the sum (7) are equal to zero. Since $1, 2, \ldots, n$ is an even permutation, $D(A) = +1$. (*b*) To prove that the condition (*b*) holds for D(A), we prove at first that D(A) satisfies prop.4. If in A the lower indices i and k are interchanged, the terms in (7) are not altered, but every even permutation becomes odd and conversely ; hence D(A) is transformed into D(A). If $\alpha_i = \alpha_k$, the exchange of i and k cannot alter D(A) ; hence $D(A) = -D(A) = 0$. If in A the column-vector α_m is replaced by $\alpha_m + \alpha_k$, in every term $a^k{}_1 \ldots a^q{}_n$ the factor $a^r{}_m$ is replaced by $a^r{}_k + a^r{}_m$, and the term is therefore increased by $a^k{}_1 \ldots a^r{}_k \ldots a^q{}_r$. The sum of these additional terms taken with the corresponding sign $\pm$ is equal to the determinant which is got when α_m is replaced by α_k.

Hence D(A) is replaced by $D(A) + \det(\alpha_1, \ldots, \alpha_k, \ldots, \alpha_k, \ldots, \alpha_n) = D(A)$. Hence the theorem.

The propositions 1 to 10 which have been established under the supposition that a function satisfying the conditions (*a*), (*b*), (*c*) exists, hold therefore unconditionally. It follows furthermore from prop.10 that this function (the determinant) is uniquely determined.

Proposition 11. $\quad \Sigma\, a^k{}_j\, A^k{}_i = 0$, for $j \neq i$. (8)

Proof. If α_i is replaced by α_j in A, the determinant is zero. Hence (8) follows from (5).

Proposition 12. Let $\alpha_1, \dots, \alpha_n$ be the column-vectors, $\alpha^1, \dots, \alpha^n$ be the row-vectors of A, then

$$\det(\alpha_1, \dots, \alpha_n) = \det(\alpha^1, \dots, \alpha^n). \tag{9}$$

Proof. In every term $a^h{}_1 \dots a^q{}_n$ of (7) the factors can be ordered in such a way that the upper indices have their natural order $1, \dots, n$; then the order of the lower indices is the inverse permutation of $h, \dots, q$. A permutation is odd (even) when its inverse permutation is odd (even). Hence

$$\det(A) = \Sigma \pm \Sigma\, a^1{}_j \, \dots \, a^n{}_p,$$

where $j, \dots, p$ takes all the permutations of $1, \dots, n$, and the sign $\pm$ has to be taken according as the permutation is even or odd. Hence $\det(A) = \det(\alpha^1, \dots, \alpha^n)$.

From this proposition it follows that in every proposition which holds for determinants, we may exchange the column-vectors and the row-vectors (i.e. the upper and the lower indices). This duality of rows and columns in a determinant can be extended to the cofactors $A^k{}_i$ by the help of the following proposition :

Proposition 13. If one replaces in the matrix A the element $a^k{}_i$ by the value 1 and those elements which are in the same row or in the same column as $a^k{}_i$ by 0, the determinant of this matrix is equal to

$$A^k{}_i = \det(\alpha_1, \dots, \alpha_{i-1}, \varepsilon^k, \alpha_{i+1}, \dots, \alpha_n) = \det(\alpha^1, \dots, \alpha^{k-1}, \varepsilon^i, \alpha^{k+1}, \dots, \alpha_n). \tag{10}$$

Proof. Let α_i be replaced by ε^k, then every term $a^1{}_1 \dots a^g{}_i \dots a^q{}_n$ of (7) is zero unless $g = k$. Since therefore in every non-vanishing term the factor a occurs, no factor $a^k{}_j$, $j \neq i$ can occur. Hence $A^k{}_i$ is independent of the elements $a^k{}_j$, which may therefore be replaced by any value, e.g. by zero. In exactly the same manner it can be proved that if in A the row α^k is replaced by the n-vector ε^i, the determinant becomes independent of $a^g{}_i$, for $g \neq k$. Hence the proposition. The essence of some of the propositions proved in this article is given by the following theorem and the subsequent formulas.

Theorem 2. det A is a linear function of its row-vectors (its column-vectors). It is invariant to row-addition (column-addition), to even permutation of the rows (columns) and to the interchanging of the rows with the columns with the corresponding index. det A changes its sign only, if an odd permutation of the rows (the columns) is performed. If rank A $< n$, then det $A = 0$.

$$\begin{aligned}\det A &= \det(\alpha_1, \ldots, \alpha_n) = \det(\alpha^1, \ldots, \alpha^n)\\ &= \Sigma \pm a^g{}_1 \ldots a^q{}_n = \Sigma \pm a^1{}_j \ldots a^n{}_p.\\ \Sigma\, a^k{}_j\, A^k{}_i &= \Sigma\, a^j{}_k\, A^i{}_k = 0 \text{ for } j \neq i \\ &= \det A \text{ for } j = i. \end{aligned} \tag{11}$$

1-9. *The Minors of a determinant.*

Again, let A be a matrix with n rows and n columns. It has been proved in 1-8 prop.3, and theorem 2, that if the columns of A are dependent and therefore the rows are dependent, then det $A = 0$. It is important to know that the converse holds too, *i.e.* that if the determinant is zero, the columns (and the rows) are dependent. Of course if det $A = 0$, then 1-8 (11) shows that $\Sigma\, \alpha^k A^k{}_i = \Sigma\, \alpha_k A^i{}_k = 0$, for $i = 1, \ldots, n$. Hence the columns (the rows) are dependent; only in the case when every $A^k{}_i$ is zero, this conclusion fails. To get a general proof, one has to go somewhat deeper into the matter. Consider:

$A^1{}_1 = \Sigma \pm a^1{}_1\ a^g{}_2 \ldots a^q{}_n$, where $a^1{}_1 = 1$, since $\begin{pmatrix} 2, \ldots, n \\ g, \ldots, q \end{pmatrix}$ is an even or odd permutation according as $\begin{pmatrix} 1, 2, \ldots, n \\ 1, g, \ldots, q \end{pmatrix}$ is. Hence

$$A^1{}_1 = \Sigma \pm a^g{}_2 \ldots a^q{}_n,$$

where + has to be taken for the even permutations of $2, \ldots, n$, and − for the odd ones. Hence $A^1{}_1$ is the determinant of the matrix which is generated by striking out the first row and the first column of A. Similarly the determinant $A^k{}_i$ is generated by replacing $a^k{}_i$ by 1 and putting 0 for the other elements in the k^{th} row and for those in the i^{th} column. The k^{th} row may be interchanged by a simple transposition with the $(k-1)^{st}$, then with the $(k-2)^{nd}$ etc. Thus by $k-1$ transposition the k^{th} row is displaced to the first place, the relative order of the remaining rows not being altered. By this operation $A^k{}_i$ takes the factor $(-1)^{k-1}$. Subsequently the i^{th} column is moved to the first place, and $A^k{}_i$ is therefore replaced by $(-1)^{i+k} A^k{}_i$. Then the first element of the first row is equal to 1, whereas the other elements of the first row and of the first column are equal to zero. As has been shown above, these two lines can be omitted without altering the determinant. Hence:

Proposition 1. $(-1)^{i+k} A^k_i$ is equal to the determinant which is generated when the row and the column which intersect in a^k_i are both omitted.

Definition. Let B be a matrix with m rows and n columns. If one omits $m - r$ rows and $n - r$ columns, the determinant of the remaining square-shaped matrix multiplied with $\epsilon = \pm 1$ is called a *minor* of B of order r.

E.g. let A be a square-shaped matrix; its minors of highest possible order are det A and $-$ det A. From prop.1 it follows that the cofactors of the elements of a square-shaped matrix are minors. By permutations of the rows and of the columns, a minor is transformed into a minor as this permutation means a multiplication with ± 1 only. Let $k_1, \ldots, k_r$ be $r < n$ different numbers. If $a_{i_1}, \ldots, a_{i_r}$ are replaced in det $(a_1, \ldots, a_n)$ by $\epsilon^{k_1}, \ldots, \epsilon^{k_r}$, one gets a determinant

$$A^{k_1, \ldots, k_r}_{i_1, \ldots, i_r} \tag{1}$$

By applying r times prop.1, it follows:

Proposition 2. The determinant (1) is a minor of A, and it is generated by omitting in A the rows $k_1, \ldots, k_r$ and the columns $i_1, \ldots, i_r$; the determinant of the remaining matrix multiplied by $\epsilon = \pm 1$ is equal to the determinant (1). ϵ is equal to $+1$, or -1 according as $i_1 + \ldots + i_r + k_1 + \ldots + k_r$ is even or odd.

As det A is a linear and homogeneous function of minors of order $n - 1$ [see 1-8, prop.9], det A$=0$ if every minor of order $n-1$ is equal to zero. Similarly, if every minor of order $n-2$ is equal to zero, the same holds for every minor of order $n-1$ and therefore for det A. By repeated application of this consideration one gets the following result:

Proposition 3. If every minor of order m is equal to zero, then the same holds for the minors of higher order.

The rank of a matrix is equal to zero if and only if every element is equal to zero, i.e. if every minor of order 1, and therefore every minor is equal to zero. The connection between the rank of a matrix and the maximum order of non-vanishing minors will be investigated now.

Proposition 4. Let B be a matrix with $m \leqq n$ rows and n columns. If a minor of B of order m is different from zero, rank B $= m$.

Proof. Let the minor composed of the m column-vectors $\alpha, \dots, \rho$ be different from zero; then these m-vectors are independent [see 1·8, prop. 3]. Hence rank B = rank C(B) = m.

If $m > n$, and a minor of B of order n is different from zero, the matrix can be transformed by interchanging of rows and columns to the case considered in prop. 4. Hence rank B = n.

Theorem. If B has a minor of order r which is different from zero, but every minor of higher order (if any) is equal to zero, then rank B = r.

Proof. Since the rank of a matrix is not altered by permutations of rows and of columns, we suppose without loss of generality that the determinant formed by the rows $1, \dots, r$ and the columns $1, \dots, r$ is different from zero. Thus the matrix formed by the rows $1, \dots, r$

$$\begin{matrix} a^1_1, \dots, a^1_r, \dots, a^1_n \\ \dots\dots\dots\dots\dots\dots \\ a^r_1, \dots, a^r_r, \dots, a^r_n \end{matrix}$$

is of rank r, and the row-vectors $\alpha^1, \dots, \alpha^r$ are therefore independent. Consider the matrix formed by $\alpha^1, \dots, \alpha^r, \alpha^v$, $r < v \leq n$, and for any particular, v, consider those minors of order $r+1$ which contain the columns $1, \dots, r$.

$$\begin{matrix} a^1_1, \dots, a^1_r, \dots, a^1_u, \dots, a^1_n \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a^r_1, \dots, a^r_r, \dots, a^r_u, \dots, a^r_n \\ a^v_1, \dots, a^v_r, \dots, a^v_u, \dots, a^v_n. \end{matrix}$$

Each of these minors is equal to zero, and the cofactors, say

$$A^1, \dots, A^r, A^v \quad \text{of}$$

$$a^1_u, \dots, a^r_u, a^v_u$$

have the same values for every u; they are minors cut out of the columns $1, \dots, r$. In particular

$$A^v = \begin{vmatrix} a^1_1, \dots, a^1_r \\ \dots\dots\dots\dots \\ a^r_1, \dots, a^r_r \end{vmatrix} \neq 0.$$

Hence $$A^1 a^1_k + \dots + A^r a^r_k + A^v a^v_k = 0$$

holds for $k = 1, \dots, r, \dots, n$. Hence

$$A^1 \alpha^1 + \dots + A^r \alpha^r + A^v \alpha^v = 0.$$

Since $A^v \neq 0$, the n-vector a^v is dependent on $a^1, \ldots, a^r$. This holds for $v = r + 1, \ldots, n$. Hence $a^1, \ldots, a^r$ form a basis of the vectorspace R(B) generated by the rows of B. Hence rank $B = r$.

If therefore A has n rows and n columns and $\det A = 0$, then rank $A < n$, i.e. the rows (columns) are dependent.

1·9. *Generalised cofactors.*[*] By the formula $\det A = \sum_k a^i_k A^i_k$, the determinant is expressed as the scalar product of the n-vector $(a^i_1, \ldots, a^i_n)$ and the n-vector $(A^i_1, \ldots, A^i_n)$; thus det A is represented as a function which is linear in two different sets of variables (*bilinear* function), one set consisting of minors of order 1, the other set consisting of minors of order $n - 1$. This representation can be generalised to a representation as a bilinear function by one set of minors of order m and one set of minors of order $n - m$. For this purpose the indices $1, \ldots, n$ are subdivided into two portions $1, \ldots, m$ and $t, \ldots, n$ where $1 < m$, and $m + 1 = t < n$. Every term of $\det A = \sum \pm a^1_j \ldots a^n_p$ can be represented as the product of two terms

$$\pm a^1_j \ldots a^n_p = (-1)^\varepsilon a^1_r \ldots a^m_s . \quad (-1)^\delta a^t_{r'} \ldots a^n_{s'}, \tag{1}$$

where $\varepsilon + \delta$ is even or odd according as $r, \ldots, s, r', \ldots, s'$ is an even or an odd permutation of $1, \ldots, n$. Every term generates a partition of the lower indices into two classes, one class $r, \ldots, s$ of m elements and one class $r', \ldots, s'$ of $n - m$ elements.

There exist $\binom{n}{m}$ such partitions; each partition corresponds to $m!\,(n - m)!$ terms of the determinant, as the elements of the first class admit $m!$ permutations. Of course $\binom{n}{m} m!\,(n - m)! = n!$ is the number of the terms of the determinant. Consider at first the partition, where

$$\begin{aligned} r, \ldots, s &= 1, \ldots, m \\ r', \ldots, s' &= t, \ldots, n, \quad t = m + 1. \end{aligned} \tag{2}$$

---

[*] This section may be omitted at a first reading.

[‡] The expansion of a determinant given in 1·9, (5) is named after Laplace.

Put $\epsilon = 0$ or $= 1$ according as the permutation of $r, \ldots, s$ is even or odd. Since $\epsilon + \delta$ is even or odd according as $r, \ldots, s, r', \ldots, s'$ is an even or an odd permutation, δ is even or odd according as $r', \ldots, s'$ is even or odd. The sum of these terms is equal to

$$\Sigma (-1)^{\epsilon} a^{1}_{r} \ldots a^{m}_{s} \ \Sigma (-1)^{\delta} a^{t}_{r'} \ldots a^{n}_{s'} = A^{1, \ldots, n}_{r, \ldots, s} A^{t, \ldots, m}_{r', \ldots, s'}. \tag{3}$$

An arbitrary even permutation of the lower indices of the product on the left band side of (1) transforms this term into another term of the determinant without altering the sign + or − . Let now

$$r, \ldots, s, \ r', \ldots, s' \tag{4}$$

be an even permutation of the indices $1, \ldots, n$, then the terms

$$(-1)^{\epsilon+\delta} a^{1}_{r} \ldots a^{m}_{s} a^{t}_{r'} \ldots a^{n}_{s'}$$

which one gets by multiplying the two sums on the left hand side of (3) are terms of the determinant, each with the correct sign + or −. If by the permutation of the indices, dashed indices are exchanged with non-dashed ones, none of these terms will be a term of (3). Therefore one gets the $n\,!$ terms of the determinant with the correct signs each once and only once in the following manner: One performs all the $\binom{n}{m}$ different partitions of the indices $1, \ldots, n$ into m indices without dash and $n-m$ indices with dash; one arranges the dashed and the non-dashed indices in such a manner that (4) is an even permutation, and one forms the product (3). This product contains the $m!(n-m)!$ terms of the determinant corresponding to the partition. The sum of all these products is equal to the determinant.

Hence

$$\det A = \sum A^{1, \ldots, m}_{r, \ldots, s} \ A^{t, \ldots, n}_{r', \ldots, s'}, \tag{5}$$

where the sum has to be taken, as explained above.

Since an even permutation of the rows does not alter the determinant, the upper indices $1, \ldots, m, t, \ldots, n$ (where $t = m + 1$) can be replaced by any particular even permutation of these terms. This permutation must be the same for all the terms of (5). If the permutation is an odd one, the sum (5) is equal to − det A ; if the upper indices are not all different, the sum is equal to zero.

1·10. *Solution of systems of linear equations by the help of determinants.*

Consider m linear equations with n variables

$$
\begin{array}{c}
a^1_1 x_1 + \dots + a^1_n x_n = a^1_0 \\
\dots\dots\dots\dots\dots\dots\dots\dots \\
a^n_1 x_1 + \dots + a^n_n x_n = a^n_0.
\end{array}
\tag{1}
$$

Multiply the equations with the cofactors of the k^{th} column and add ; then $x_k \det A = \sum_i a^i_0 A^i_k = \det(\alpha_1, \dots, \alpha_0, \dots, \alpha_n)$, where in the determinant on the right hand side, α_0 stands on the k^{th} place. If $\det A \neq 0$,

$$
x_k = \det(\alpha_1, \dots, \alpha_0, \dots, \alpha_n) : \det A, \tag{2}
$$
$$
\text{for } k = 1, \dots, n.
$$

This condition is necessary, but as there exists a solution and $x_1, \dots, x_n$ is uniquely determined by (2), the condition is sufficient too. Verify this result by putting (2) into (1).

$$
\sum_k a^j_k x_k = \{ \sum_k a^j_k \sum_i a^i_0 A^i_k \} : \det A = \{ \sum_i a^i_0 \sum_k a^j_k A^i_k \} : \det A,
$$

$$
\begin{aligned}
\text{but } \sum_k a^j_k A^i_k &= \det A \text{ for } j = i \\
&= 0 \text{ for } j \neq i \text{ ; hence}
\end{aligned}
$$

$$
\sum_r a^j_k x_k = a^j_0.
$$

As this result holds for $j = 1, \dots, m$, the equations (1) are satisfied by (2). For the case when the number of the equations is different from the number of the unknown quantities, the method needs some modification. If the rank of the full matrix is greater than the rank of the homogeneous portion, the system has no solution. Let the two ranks be equal, and equations depending on the other ones be omitted. The rank of the matrices is therefore supposed to be equal to the number m of the equations

$$
\begin{array}{c}
a^1_1 x_1 + \dots + a^1_m x_m + \dots + a^1_n x_n = a^1_0 \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
a^m_1 x + \dots + a^m_m x_m + \dots + a^m_n x_m = a^m_0.
\end{array}
\tag{3}
$$

There exists therefore a determinant formed by m columns of the coefficients on the left hand side which is different from zero. Without loss of generality, suppose that it is the determinant

$$
\begin{vmatrix}
a^1_1, \dots, a^1_m \\
\dots\dots\dots \\
a^m_1, \dots, a^m_m
\end{vmatrix}
= d \neq 0.
$$

Multiplying the equations with the cofactors of the k^{th} column ($k=1, \dots, m$) and dividing by d, one gets .

$$x_k = d_{k,o} + d_{k,m+1}\, x_m + \dots + d_n\, x_n,\quad k = 1, \dots, m, \tag{4}$$

where $d_{k,o} = \quad \det(\alpha_1, \dots, \alpha_o, \dots, \alpha_m)$

$$d_{k,\mu} = -\det(\alpha_1, \dots, \alpha_\mu, \dots, \alpha_m),\ \mu = m+1, \dots, n.$$

In the determinants on the right hand side, α_o and α_μ are supposed to be put in the k^{th} place.

1-(10)1. *Comparison of the different methods for solving systems of linear equations.* Three methods for solving linear equations have been discussed : "Sweep out", "orthogonalisation", and "determinants" ; furthermore the method of "substitution" has been mentioned in the introduction. Common features of these methods are the following :

(1) A given system of linear equations, say 1-10, (1) or (3) is replaced by another one which either gives the solution, if there exists one only, [see 1-10, (2)] or shows a method of finding any number of solutions [see 1-10, (4)], if there exist more solutions than one.

(2) The derived linear equations are homogeneous linear combinations of the original equations, such that if the original equations are satisfied, the derived equations hold. I.e. the derived equations are *necessary* conditions.

(3) The original linear equations are homogeneous linear combinations of the derived ones. Hence the derived equations are *sufficient* conditions. By the method of "sweep out" as well as by the method of substitution, this reduction of the given linear equations is done step by step. Consider the method of substitution.

$$\begin{aligned} a(x) &\equiv a_1 x_1 + \dots + a_n x_n - a_o = 0 \\ b(x) &\equiv b_1 x_1 + \dots + b_n x_n - b_o = 0 \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ k(x) &\equiv k_1 x_1 + \dots + k_n x_n - k_o = 0 \end{aligned}$$

The symbols on the left hand side are only abbreviations for the linear functions in the centre.

If $a_1 \neq 0$, $x_1 = [a_0 - a_2 x_2, \ldots, - a_n x_n] : a_1$. By putting this value into the other equations, we get equations of the type

$$\left(b_2 - \frac{b_1 a_2}{a_1}\right)x_2 + \ldots + \left(b_n - \frac{b_1 a_n}{a_1}\right)x_n - \left(b_0 - \frac{b_1 a_0}{a_1}\right) = 0.$$

This equation is identical with $b(x) - \frac{b_1}{a_1} a(x) = 0$. Thus this "putting in" means the same as the "sweep out" of the first column. By the help of one of these new equations, x_2 is represented as a function of $x_3, \ldots, x_n$; this value is put into the remaining $n - 2$ equations; thus the second column is swept out in $n - 2$ rows. The substitution leads after $n - 1$ steps to a system of the following type (provided the rank of the matrix of the homogeneous portion is equal to n):

$$\begin{aligned} a_1 x_1 + \qquad \ldots + a_n x_n - a_0 &= 0 \\ c_2 x_2 + \ldots + c_n x_n - c_0 &= 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ t_n x_n - t_0 &= 0. \end{aligned}$$

The matrix is swept out *below* the diagonal. By putting $x_n = t_0 : t_n$ into the other equations the n^{th} column is swept out. The $(n-1)^{st}$ equation is transformed to $s\, x_{n-1} - s_0 = 0$; putting $x_{n-1} = s_0 : s$ into the other equation the $(n-1)^{st}$ column is swept out, etc. Finally the matrix is completely swept out and the values of $x_1, \ldots, x_n$ are determined.

The method of substitution is therefore not essentially different from the method of sweep out. The method of determinants does not use a procedure by steps. One determines numbers A, B, ..., K such that

$$\mathrm{A}\, a(x) + \mathrm{B}\, b(x) + \ldots + \mathrm{K}\, k(x)$$

is independent of $x_2, \ldots, x_n$, and is therefore of the type

$$u\, x_1 - v = 0, \text{ or } x_1 = v : u.$$

This condition is necessary, but it may not be a sufficient one. In the preceding sections it has been shown, that by the method of determinants one gets necessary and sufficient conditions for the unknown quantities $x_1, \ldots, x_n$, in a suitable form, provided the fundamental condition for the ranks of matrices holds [see 1-6, theorem 2.]. For numerical calculation it is sometimes useful to use methods of elimination and of "sweep out" jointly. When one proceeds on this way, it is advisable to consider very carefully whether the necessary conditions stated in this manner are also sufficient.

In general, the methods of determinant and of orthogonalisation are not very suitable for numerical calculation. To calculate a determinant, it is in general not advisable to determine the $n\,!$ terms of 1-8, (7), but to simplify the determinant by sweeping out the matrix below or above the diagonal. The value of the determinant is then equal to the product of the elements in the diagonal. A determinant can be swept out by row-addition as well as by column-addition. In some cases it is useful to calculate a determinant by the help of 1-8, (5).

1-(11). *Linear transformations.* In the preceding sections, the n-vector

$$\xi = (x_1, \ldots, x_n) \tag{1}$$

has been considered as an unknown quantity, whereas the coefficients were supposed to be given numbers. For many applications of the theory (*e.g.* application to Geometry), it is necessary to investigate the mutual connection between the numbers, n-vectors and matrices occuring in these formulas.

Consider

$$\begin{aligned} a^1{}_1\, x_1 + \ldots + a^1{}_n\, x_n &= y_1, \\ \cdots\cdots\cdots\cdots&\cdots\cdots \\ a^n{}_1\, x_1 + \ldots + a^n{}_n\, x_n &= y_n\,; \end{aligned} \tag{2}$$

then to every n-vector ξ, there corresponds an n-vector

$$\eta = (y_1, \ldots, y_n). \tag{3}$$

This correspondence will be denoted by an arrow

$$\xi \to \eta. \tag{4}$$

This formula may be read : *A transforms ξ into η.* The formula (2) is called a *linear transformation.* From (2) it follows (the same notations as in previous sections being used) :

$$0 \to 0 \tag{5}$$

$$e^k \to a_k. \tag{6}$$

If $$\xi_j \to \eta_j, \quad j = 1,\ 2, \ldots,$$

then $$c_1\, \xi_1 + \ldots + c_m\, \xi_m \to c_1\, \eta_1 + \ldots + c_m\, \eta_m. \tag{7}$$

Hence, if ξ takes all the n-vectors of a vectorspace V, the corresponding vectors form a vectorspace V', as from $\xi \to \eta$, $\xi' \to \eta'$ it follows, that $\xi + \xi' \to \eta + \eta'$ and $c\ \xi \to c\ \eta$ [see 1-3, prop.10]. A system of dependent n-vectors is transformed into a system of dependent n-vectors, but the converse may not hold.

Let V be a complete vectorspace of rank n, then $\xi = (x_1, \ldots, x_n) = x_1 \varepsilon^1 + \ldots + x_n \varepsilon^n$. Hence $\xi \to x_1 \alpha_1 + \ldots + x_n \alpha_n$. Every vector of V' can be represented in this manner, and $x_1, \ldots, x_n$ take independently all values, V' is therefore generated by $\alpha_1, \ldots, \alpha_n$ and rank V' = rank A. Hence :

Theorem 1. By a linear transformation (2) a vectorspace is transformed into a vectorspace and the vectorspace of rank n is transformed into a vectorspace of a rank equal to rank A.

The notion of linear transformation can fully be characterised by the manner how sums of vectors and products of numbers and vectors are transformed. This fact is shown by the following theorem.

Theorem 2. If the n-vectors (1) are represented by n-vectors (3) in such a manner that to the sum of two vectors there corresponds the sum of the corresponding vectors and that to the product of a number c and an n-vector there corresponds the product of c and the corresponding n-vector, then the representation is effected by a linear transformation.

Proof. Let $\alpha_k = (a^1{}_k, \ldots, a^n{}_k)$ be the n-vectors which represent the unit-vectors ε^k $(k = 1, \ldots, n)$. Then $x_k \varepsilon^k$ is represented by $x_k \alpha_k$, and $\xi = (x_1, \ldots, x_n) = \Sigma\, x_k \varepsilon^k$ is represented by $\Sigma\, x_k \alpha_k$, *i.e.* by the n-vector η which is determined by (2) and (3). Hence the theorem.

1-(11)1. *Composition of transformations. Product of matrices.* Let ξ be transformed into η by 1-(11), (2) and η be transformed into ζ by another linear transformation.

$$\begin{array}{c} b^1{}_1\, y_1 + \ldots + b^1{}_n\, y_n = z_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b^n{}_1\, y_1 + \ldots + b^n{}_n\, y_n = z_n. \end{array} \qquad (1)$$

The matrix $((b^k{}_j))$ will be denoted by B.

Then
$$z_k = \sum_j b^k{}_j\, y_j = \sum_{j,s} b^k{}_j\, a^j{}_s\, x_s = \Sigma\, g^k{}_s\, x_s, \qquad (2)$$
$$\text{where} \quad g^k{}_s = \Sigma\, b^k{}_j\, a^j{}_s.$$

Thus ξ is transformed into ζ by a linear transformation which is said to be *composed* of the transformations $\xi \to \eta$ and $\eta \to \zeta$. The matrix $((g^k{}_s)) = \mathrm{G}$ is said to be the *product*

$$\mathrm{G} = \mathrm{B\,A}.$$

To get the elements $g^k{}_s$ of G, one must multiply the elements of the k^{th} row of B with the corresponding elements of the s^{th} column of A, and add the products. In terms of scalar product [see 1·7]:

$$g^k{}_s = \beta^k\, \alpha_s,$$

where β^k denotes the k^{th} row-vector of B.

In general A B and B A are different matrices; i.e. the commutative law does not hold for the multiplication of matrices.

Let $\qquad \mathrm{C} = ((c^i{}_k)) \qquad$ be an arbitrary matrix

$$\mathrm{CB} = \mathrm{H} = ((h^i{}_j)), \text{ where } h^i{}_j = \sum_k c^i{}_k\, b^k{}_j$$

$$\mathrm{HA} = \mathrm{P} = ((p^i{}_s)) \quad \text{''} \quad p^i{}_s = \sum_j h^i{}_j\, a^j{}_s = \sum_{j,k} c^i{}_k\, b^k{}_j\, a^j{}_s$$

$$\mathrm{CS} = \mathrm{Q} = ((q^i{}_s)) \quad \text{''} \quad q^i{}_s = \sum c^i{}_k\, g^k{}_s = \sum_{j,k} c^i{}_k\, b^k{}_j\, a^j{}_s.$$

Hence P = Q, i.e.

$$(\mathrm{CB})\mathrm{A} = \mathrm{C}(\mathrm{BA}). \tag{3}$$

This formula can be expressed as a theorem.

Theorem: For the multiplication of matrices the associative law holds.

1·(11)11. *n-vectors considered as matrices.* It is often useful to consider an n-vector

$$\xi = (x_1, \ldots, x_n)$$

as a matrix, e.g. as a matrix

$$(x) = \begin{pmatrix} x_1 & 0, \ldots, 0 \\ x_2 & 0, \ldots, 0 \\ \ldots & \ldots\ldots \\ x_n & 0, \ldots, 0 \end{pmatrix}, \tag{1}$$

where the first column is formed by the coordinates of ξ, whereas the other elements are equal to zero. If we multiply such a matrix from the left hand side with an arbitrary matrix with n rows and columns, the result is again a matrix of the type (1). The linear transformation 1·(11), (2) can therefore be expressed as an equation for matrices

$$\mathrm{A}(x) = (y).$$

Similarly 1-(11)1, (1) is equivalent to

$$B(y) = (z).$$

By putting in, one gets the equation

$$BA(x) = z,$$

which expresses 1-(11)1, (2) in a matrix form.

1-(11)12. *Special matrices.* A *diagonal-matrix* is a square shaped matrix, the elements of which are equal to zero, except those in the diagonal.

$$D = ((d^i_k)), \quad d^i_k = 0, \text{ if } i \neq k$$
$$d^i_i = d_i.$$

Hence

$$DA = \begin{pmatrix} d_1 a^1_1 & d_1 a^1_2, \dots, d_1 a^1_n \\ \dots\dots & \dots\dots\dots\dots \\ d_n a^n_1 & d_n a^n_2, \dots, d_n a^n_n \end{pmatrix} \tag{1}$$

$$AD = \begin{pmatrix} d_1 a^1_1 & d_2 a^1_2, \dots, d_n a^1_n \\ \dots\dots & \dots\dots\dots\dots \\ d_1 a^n_1 & d_4 a^n_2, \dots, d_n a^n_n \end{pmatrix}. \tag{2}$$

An *elementary matrix* is a square shaped matrix

$$E_{rs}(\lambda) = ((e^i_k)), \quad r \neq s,$$
$$\text{for which } e^i_i = 1 \quad (i = 1, \dots, n)$$
$$e^r_s = \lambda$$
$$e^i_k = 0, \text{ for } i \neq k, \text{ and } (i, k) \neq (r, s).$$

To multiply A from the left with $E_{rs}(\lambda)$, means a row-addition in A, by which the row α^r of A is replaced by $\alpha^r + \lambda\, \alpha^s$. To multiply A from the right with $E_{rs}(\lambda)$, means a column-addition in A, by which the column α_s of A is replaced by $\alpha_s + \lambda\, \alpha_r$.

1-(11)2. *Decomposition of Matrices.* By the method of sweep out, it has been shown that every matrix can be transformed into a matrix of a special type by row-addition, row-omission and row-multiplication [see 1-4, theorem 1]. In a similar way, it will now be shown that a square shaped matrix can be transformed into a diagonal-matrix by row-addition and column-addition. In terms of matrix-multiplication this proposition can be enounced as follows :

Theorem. Every square shaped matrix A can be represented as a product

$$A = P_1 \, D \, P_2, \tag{1}$$

where P_1 and P_2 are products of elementary matrices, and D is a diagonal-matrix.

Proof. If the matrix is the zero-matrix, then it is already a diagonal-matrix, otherwise one can arrange by column-addition (if necessary) that at least one element in the first column is different from zero, and by row-addition that $a^1{}_1 \neq 0$. Thus one can sweep out the first column by row-addition, and subsequently one can sweep out the first row by column-addition without altering the first column. If the matrix is not already a diagonal-matrix, one can arrange now by row-and column-additions without altering the first row and the first column that $a^2{}_2 \neq 0$; then the second column and the second row are swept out. This procedure can be continued up to the matrix is made a diagonal-matrix D. As every row-addition means a multiplication with an elementary matrix from the left, and similarly a column-addition corresponds to an elementary-matrix as a right hand side factor, formula (1) holds.

A representation of A as a product of diagonal-and elementary matrices is also called a *decomposition* of A into these factors.

1-(11)3. *The determinant of a matrix product.* Let D be a diagonal-matrix, then

$$\det D = d_1 \ldots d_n \det (e^1, \ldots, e^n) = d_1 \ldots d_n. \tag{1}$$

As a multiplication with an elementary-matrix from the left (right) hand side means a row-(column) addition only, the multiplication with elementary matrices, or with products of them, does not alter the determinant. Whereas by the multiplication of any matrix by D, the determinant is multiplied by det D as is seen from 1-(11)12, (1) and (2).

Hence, if $\quad A = P_1 D P_2$, then $\det A = d_1 \ldots d_n$.

Consider AB.

$$\det AB = \det DP_2B$$

$$\det P_2B = \det B$$

$$\det AB = \det D(P_2 B) = d_1 \ldots d_n \det P_2 B = \det A \det P_2 B$$
$$= \det A \det B.$$

Hence
$$\det A B = \det A \det B. \tag{2}$$

1-(11)4. *The inverse of a linear transformation.*

$$\text{By } A(x) = (y) \tag{1}$$

the n-vectors (x) are transformed into the vectors (y). If det A $= 0$, then the rank of the vectorspace generated by the n-vectors (y) is less than n, and therefore the (x) are not generated by a linear transformation of the n-vectors (y). Let det A $\neq 0$. Then $\det A \, x_k = \sum_i A^i_k \, y_i$ holds. Hence

$$A' \, (y) = (x),$$

where

$$A' = \begin{pmatrix} b^1{}_1, \ldots, b^1{}_n \\ \cdots\cdots\cdots\cdots \\ b^n{}_1, \ldots, b^n{}_n \end{pmatrix} \tag{2}$$

and $b^i{}_k = A^k{}_i : \det A$.

$$A \, A' \, (y) = (y).$$

Hence AA′ is a transformation which transforms every n-vector into itself. Let C be any matrix. $C \, (\varepsilon^i)$ is an n-vector which is equal to the i^{th} column of C. If therefore $C(\varepsilon^i) = (\varepsilon^i)$, then C is the diagonal matrix

$$E = \begin{pmatrix} 1 \; 0, \ldots, 0 \\ 0 \; 1, \ldots, 0 \\ 0 \; 0, \ldots, 1 \end{pmatrix}. \tag{3}$$

Hence $\qquad A \, A' = E.$

Furthermore $\qquad A' \, A(x) = (x).$

Hence $\qquad A' \, A = E.$

The matrix A′ is said to be the *inverse matrix* of A and is mostly denoted by A^{-1}. The necessary and sufficient condition for the existence of an inverse matrix is det A $= 0$.

E is called the *unit-matrix*. For every matrix A,

$$A \, E = A = EA \tag{4}$$

holds, and

$$E = E^{-1}.$$

CHAPTER II

FUNDAMENTALS OF GENERAL ALGEBRA

2·1. *Principal Notions.*

2·11. *Fundamental laws.* Let

$$a, b, c, \ldots \tag{1}$$

be arbitrary numbers; then there exists, for every pair of them a uniquely determined number s, the *sum*

$$a + b = s \tag{2}$$

and a uniquely determined number p, the *product*

$$a\ b = p. \tag{3}$$

The operations of forming sums and products are called *addition* and *multiplication*.

These operations satisfy the following laws:

Commutative laws:

$$a + b = b + a \tag{4a}$$

$$a\ b = b\ a. \tag{4m}$$

Associative laws:

$$(a + b) + c = a + (b + c) \tag{5a}$$

$$(ab)c = a(bc). \tag{5m}$$

Laws of inverse existence: For every pair a, b there exists an x such that

$$x + a = b. \tag{6a}$$

For every pair a, b satisfying the condition

$$a \neq 0 \tag{6o}$$

there exists an y such that

$$y\ a = b. \tag{6m}$$

Distributive laws:

$$\begin{aligned}(a + b)c &= a\,c + b\,c \\ a(b + c) &= a\,b + a\,c.\end{aligned} \tag{7}$$

Though these formulas are fundamental for calculation with numbers, they do not characterise completely the notion of number. Of course in the different branches of mathematics, the word "number" is used in different senses. One speaks e.g. of natural numbers, rational numbers, complex numbers, hypercomplex numbers etc, The rational numbers as well as the real numbers and the complex numbers form three systems each of which satisfies the above conditions, whereas the system formed by the natural numbers does not satisfy the laws of inverse existence; the reader may verify it. On the other hand, in the system formed by all the analytic functions of a complex variable, all the laws mentioned before hold, though the system is not composed of numbers. In this chapter, systems of any kind will be considered where either all these laws, or some of them hold. In general, nothing will be supposed about the nature of the mathematical elements which form these systems. The essential thing is that the elements are interconnected by the help of certain operations which obey particular laws. These operations will sometimes be called *rational operations.*

2-12. *Modules.* A system of elements for which an operation satisfying the conditions (4a), (5a), (6a) of 2-11 is defined, is said to form an *abelian group* or a *module*[*]. The system formed by the rational numbers is an instance of a module ; similarly the system of the real (the complex) numbers. The vectorspaces (see 1-3) are modules of a different type ; the elements of them are n-vectors, and the addition but not the multiplication of n-vectors has been defined. Consider especially $n = 3$. The 3-vectors can be represented by vectors in the space ; thus one gets in this way modules which are formed by geomtrical entities (vectors). Moreover to every vector there corresponds a parallel displacement of the space transforming the starting point of the vector into its endpoint, and conversely to every parallel displacement of the space there corresponds one and only one vector. To the sum of two vectors $\alpha + \beta$ there corresponds the parallel displacement which is generated by performing succesively the two parallel displacements corresponding to α and to β. Thus the parallel displacements of the space form a module ; this module therefore is composed of elements which are geometrical transformations.

The intergral numbers form a module in which besides addition and subtraction also multiplication can be performed ; whereas division is possible in special cases only.

---

[*] There is no essential difference between the meaning of the two words. The term " addition " and the sign + are only notations, and there is no harm in replacing them by other words. In these cases it is unusual to speak of "modules" and the word module is replaced by " abelian group ".

The rotations about any particular axis form a module which is connected with the module of the real numbers as follows: Let g be a particular positive integral number, and let to every real number α correspond the rotation through the angle $2\pi\alpha$: g, then there corresponds a rotation to every real number, and to two real numbers α and β there corresponds the same rotation if and only if $\alpha - \beta$ is an integral multiple of g. Two rotations corresponding to the numbers κ and λ generate, if taken one after the other, a rotation which corresponds to $\kappa + \lambda$. The rotations for which α is an integral number, form a finite system which is a module. Each of these rotations corresponds to one of the integral numbers $0, 1, 2, \ldots, g - 1$, which occur as residues when an integral number is divided by g. Two integral numbers corresponding to the same rotation (and therefore to the same residue) are said to be *congruent*.

$$a \equiv b \pmod{g};$$

they form *a class of residues* modulo g. It will be proved later on that these classes form a module; this module is of a special interest, especially in the case when g is a prime number.

2·13. *Partition into classes.* In the example considered just before, a partition of the set of all integers into classes has been generated by a congruence of its elements. This consideration will now be generalised.

An arbitrary set A of elements $a, b, c, \ldots$ may be decomposed into classes, so that every element belongs to one and only one class. Two elements are said to be *equivalent*, written $a \sim b$, if they belong to the same class. Then the equivalence has the following properties:

$$\begin{array}{lll} a \sim a & \text{law of reflexivity.} & \\ \text{If } a \sim b, \text{ then } b \sim a & \text{law of symmetry.} & (1) \\ \text{If } a \sim b, b \sim c, \text{ then } a \sim c & \text{law of transitivity.} & \end{array}$$

Hence to every partition of a set A into classes, there corresponds an equivalence of its elements, such that the three laws (1) are satisfied for this equivalence. The usual way of mathematical investigation however is the converse one: An equivalence between the elements of A is given, and from this equivalence, a partition into classes is derived. It has been shown just before that an equivalence which generates a partition into classes must satisfy the conditions (1); by the following lemma it will be established that these conditions are not only necessary, but also sufficient for a partition into classes.

Lemma. Given an equivalence between the elements of A satisfying the condition (1), and let (a) (b), (c), ... be the classes of the elements equivalent respectively to $a, b, c, \ldots$, then each element of A belongs to a class, and two classes have either all elements in common—*i.e.*, they are identical — or they have no common element.

Proof. As $a \sim a$, the element a itself belongs to the class (a), formed by the elements equivalent to (a). If b is a common element of (a) and (c), then it follows from the law of symmetry that a and c belong to (b). From the law of transitivity it follows that each element of (a) and of (c) belongs to (b), and that each element of (b) belongs to (a) and to (c). Therefore (a), (b) and (c) are identical.

Each element of a class will be called its *representative*, and we will use the notation :

$$(a) = \text{the class represented by } a. \tag{2}$$

By the method of forming classes, often new mathematical entities are created. From the operations on the original elements, operations on the classes are derived in the following manner :

Let an operation, say addition, exist for the elements of any system A, and let a partition of A into classes be given. The sum of two classes is mostly defined by

$$(c) + (d) = (c + d). \tag{3}$$

But this definition is admissible if and only if the class $(c + d)$ is the same whatever elements c and d are chosen as the representatives of their classes. Similar in the case when the operation is multiplication.

Now the congruence (mod. g) defined in 2-12 is an equivalence satisfying obviously the conditions (1). This congruence generates a partition into g *classes of residues*

$$(0), (1), \ldots, (g - 1). \tag{4}$$

The lemma proved just before will be applied to these classes. As every integer is congruent to its residue after division by g, $(a) = (a')$ if and only if $a \equiv a'$ (mod. g) ; furthermore if $(a) = (a')$, $(b) = (b')$, $a' = a + r g$, $b' = b + s g$, hence $(a + b)$ and $(a' + b') = (a + b + [r + s] g)$ denote the same class. It is therefore admissible to define addition of classes by :

$$(a) + (b) = (a + b) ; \tag{5}$$

similarly : $\quad (a)(b) = (a b).$

From (5) it follows directly:

$$\begin{array}{ll} (\mathrm{a})+(\mathrm{b}) = (\mathrm{b})+(\mathrm{a}), & [(\mathrm{a})+(\mathrm{b})]+(\mathrm{c}) = (\mathrm{a})+[(\mathrm{b})+(\mathrm{c})] \\ (\mathrm{a})+(\mathrm{b}-\mathrm{a}) = (\mathrm{b}), & \\ (\mathrm{a})(\mathrm{b}) = (\mathrm{b})(\mathrm{a}), & [(\mathrm{a})(\mathrm{b})](\mathrm{c}) = (\mathrm{a})[(\mathrm{b})(\mathrm{c})] \\ [(\mathrm{a})+(\mathrm{b})](\mathrm{c}) = (\mathrm{a})(\mathrm{c})+(\mathrm{b})(\mathrm{c}), & (\mathrm{a})[(\mathrm{b})+(\mathrm{c})] = (\mathrm{a})(\mathrm{b})+(\mathrm{a})(\mathrm{c}). \end{array}$$

Hence the classes of residues (mod.g) form a module in which a second operation, the "multiplication" is defined satisfying the conditions (4m), (5m) and (7) of 2-11.

2-14. *Singular elements.* Although a module is not necessarily a set of numbers, there exists in every module an element which has about the same properties as the number zero, and which is therefore used to be denoted by the character 0.

Theorem. In a module M there exists one and only one *singular* element 0, such that for every element a of M, $a + x$ equals (does not equal) a, if x is the singular (a non-singular) element.

Proof. Let a be any particular element of M. As the law of inverse existence (6a) of 2-11 holds for the addition, as defined in M, there must exist an element, say 0 of M satisfying the condition

$$a + 0 = a. \tag{1}$$

Thus the sum of a and 0 is a itself. It will be proved now that this element 0 has the same property with respect to every element of M, and that it is unique. Let b be an arbitrary element of M, then there exists an element c of M, satisfying

$$c + a = b.$$

Hence

$$b + 0 = (c + a) + 0 = c + (a + 0) = c + a = b.$$

Hence 0, when added to any element b of M gives b.

To prove its uniqueness, one may suppose that there exists another element, say $\bar{0}$ in M, so that $a + \bar{0} = a$, then $\bar{0}$ has the same properties as 0, and the elements of M will not change, when $\bar{0}$ will be added. Hence $0 + \bar{0} = 0$, but on the other hand $0 + \bar{0} = \bar{0}$ holds. Hence $0 = \bar{0}$.

There exists in M an element a', for which

$$a + a' = 0 \tag{2}$$

holds. The uniqueness of a' is a consequence of the following consideration.

Let $c + a = \bar{c} + a = b$, then

$$c = c + 0 = c + (a + a') = b + a' = (\bar{c} + a) + a' = \bar{c} + 0 = \bar{c}.$$

Hence :

Theorem. The equation $x + a = b$ has one and only one solution.

2·15. *Operations in a module.* The addition of a' is the operation inverse to the addition of a. The addition of a' will therefore be called the *subtraction* of a, and the following notations will be used :

$$a' = -a \tag{1}$$

$$d + a' = d - a. \tag{2}$$

Since $-a' = a$, $\quad -(-a) = a$ holds.

Now $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$; hence one can omit the brackets in this sum. By mathematical induction one can prove in the same manner, as is done in elementary arithmetic, that the brackets in the sums of n elements can be omitted. In place of $a_1 + a_2 + \dots + a_n$ one writes sometimes

$$\sum_{i=1}^{n} a_i ;$$

for abbreviation this notation is often replaced by $\sum_i a_i$, or by $\sum a_i$, when there is no ambiguity.

If $a_1 = a_2 = \dots = a_n = a$, the sum will be denoted by

$$\mathrm{n}\, a ; \tag{3}$$

thus n is a *positive integer*, and *not necessarily an element of M*.

The product of a non-positive integer with an arbitrary element a of M is defined by

$$(-\mathrm{n})a = -(\mathrm{n}a) = \mathrm{n}(-a)$$

$$0\, a = 0. \tag{3'}$$

Hence for all integers p,q the following distributive laws hold :

$$\mathrm{p}a + \mathrm{q}a = (\mathrm{p} + \mathrm{q})\, a$$

$$\mathrm{p}\,(a + b) = \mathrm{p}a + \mathrm{p}b.$$

A system S' which is formed by elements of any set S is said to be a *subset* of S. In particular, a subset M' of a module (an abelian group) M is said to be a *submodule* (*a subgroup*) of M if it forms a module with respect to the addition defined in M.

Theorem. A subset M' is a submodule of M, if and only if the differences of the elements of M' belong to M'.

Proof The condition is obviously necessary. Let the condition hold, and let a and b be elements of M' then $b - b = 0$, $0 - b = -b$, and $a - (-b) = a + b$ belong to M'. Hence the addition defined in M can be carried out in M'; for this addition the associative and the commutative laws hold, and the equatation $x + a = b$ can be solved by the element $b - a$ of M'. Hence M' is a submodule of M.

2·16. *Rings.* If in a module T, a multiplication satisfying the associative and the distributive laws are defined in such a manner that the product of every pair of elements belongs to T, this module is called a *ring*, and if in a ring the multiplication satisfies the commutative law (4m) of 2·11, the ring is said to be a *commutative ring*.

The integral numbers form a commutative ring R; other instances of commutative rings are the sets R_g of the integral multiples of an integral number g, and the classes of residues (mod. g). Non-commutative rings are *e.g.* formed by matrices [see ch. VI].

A subset of a ring T, which itself is a ring with the addition and the multiplication, as defined in T as its operations, is said to be a *subring* of T.

Exercises: (1) A subset T' of a ring T is a subring of T if and only if the differences and the products of the elements of T' belong to T'.

(2) Replace the law of reflexivity by the following condition: "To every element of A there exists at least one element which is equivalent to it", and show that this condition in connection with the laws of symmetry and transitivity implies the law of reflexivity.

As the distributive law holds in a ring,

$$\begin{aligned} 0 &= cc - cc = c(c - c) = c\,0 \\ &= (c - c)c = 0\,c. \end{aligned}$$

Therefore it is impossible to satisfy the condition (6m) of 2·11 in any ring without restriction. If we want to introduce the condition that to every pair of elements a, b there should exist such an y that

$$y\,a = b,$$

we are compelled to make the restriction

$$a \neq 0.$$

We get this restriction from formula (6o) of 2·11 by replacing the number 0 by the singular element 0 of the module T; when mentioned in the following, the formula (6o) of 2·11 should always be understood in that way.

2·2. *Fields.* If in a commutative ring which contains more than one element the condition (6m) with the restriction (6o) of 2·11 holds, it is said to be a *field*. In other words: a field is a set of more than one element in which an addition and a multiplication are defined, and the conditions (4a), (4m), (5a), (5m), (6a), (6m) with (6o) and (7) of 2·11 hold for these operations.

Theorem. If a, b are elements of a field F and $a\,b = 0$, then at least one of the factors a, b must be equal to 0.

Proof. Let $a \neq 0, b \neq 0$. From (6m) and (6o) of 2·11 it follows that there is in F an element c such that $c\,b \neq 0$ (*e.g.* $c\,b = a$) and an element y such that $y\,a = c$. Then: $0 = y\,0 = y\,a\,b = c\,b \neq 0$. Hence the theorem.

From this theorem it follows, that the elements $\neq 0$ of a field F form a system Σ where the multiplication is commutative and associative, and in which for every pair a, b of elements of Σ, the equation $a\,x = b$ has a solution in Σ. Hence the multiplication satisfies in Σ the same conditions, as the addition must satisfy in a module; only the sign of $+$ has been replaced by the notation of the multiplication. So one can "translate" the results of 2·15 from the "additive language" into the "multiplicative language",

2·21. *Nullelement and Unitelement.* From 2·14 there follows the existence of a unique *singular* element 1 satisfying the condition

$$a\,1 = 1\,a = a \tag{1}$$

for every element a of Σ. But, as (1) holds also for $a = 0$, it follows:

Theorem 1. There is one and only one element 1 in a field satisfying (1) for every element a of the field.

To every element a of Σ there is an element a^{-1} satisfying

$$a\,a^{-1} = a^{-1}\,a = 1. \tag{2}$$

By translating the theorem of 2-15 into the "multiplicative language" one gets :

Theorem 2. If a and b are elements of a field F and $a \neq 0$, then the equation $a\,x = b$ has one and only one solution in F, namely $x = a^{-1}\,b$.

Corresponding to the sum of n elements one can form the product $\prod_{i=1}^{n} a_i$ of n elements, and if the elements are all equal, the product is the *power*

$$a^n. \tag{3}$$

The powers with non-positive integral exponents are defined by

$$a^0 = 1, \quad a^{-n} = (a^n)^{-1} = (a^{-1})^n.$$

Hence for every pair of integers p, q the equation

$$a^p\,a^q = a^{p+q} \tag{4}$$

holds.

The necessary and sufficient conditions which a field must satisfy, can also be given in the following manner :

A system F of more than one element, for which the addition and the multiplication are uniquely defined, is a field if and only if :

1. The elements form a module ; the singular element may be denoted by 0.
2. The elements different from 0 form a system Σ of at least one element which is an abelian group with respect to the multiplication.
3. $a\,0 = 0\,a = 0$.
4. $a\,(b + c) = a\,b + a\,c$, for arbitrary elements a, b, c of F.

The singular element 0 of the module will be called the *nullelement* or *zero-element*.

The singular element 1 of Σ will be called the *unitelement*.

$$1 \neq 0. \tag{5}$$

2-22. *Homomorphism, Isomorphism and Automorphism.* Let the elements a, b, c, ... of an arbitrary ring T be represented by the elements

$$\alpha(a),\ \alpha(b),\ \alpha(c),\ \ldots$$

of a set A, and let an addition and a multiplication exist in A for which the formulas

$$\begin{aligned} \alpha(a) + \alpha(b) &= \alpha(a+b), \\ \alpha(a)\,\alpha(b) &= \alpha\,(ab) \end{aligned} \tag{1}$$

are satisfied for all elements a, b of T, then the representation is said to be a *homomorphism* and A is said to be *homomorphic* to T. The element $\alpha(a)$ of A is said to be the *image* of the *original* element a of T. The representation of a by $\alpha(a)$ is denoted sometimes by

$$a \to \alpha(a)\ ;$$

one says that a particular homomorphism *maps* A on T. There are homomorphisms where different elements are mapped on the same image.

Theorem 1. A is a ring. If T is commutative, A is also a commutative ring.

Proof. Every element of A is of the form $\alpha(a)$, where a is a suitable element of T, not necessarily defined uniquely by its image $\alpha(a)$.

$$\begin{gathered} [\alpha(a) + \alpha(b)] + \alpha(c) = \alpha(a+b+c) = \alpha(a) + [\alpha(b) + \alpha(c)] \\ \alpha(a) + \alpha(b) = \alpha(a+b) = \alpha(b) + \alpha(a) \\ \alpha(a) + \alpha(b-a) = \alpha(b). \end{gathered} \tag{2}$$

Hence A is a module.

The nullelement of A is $\alpha(0)$, since

$$\alpha(a) + \alpha(0) = \alpha(a+0) = \alpha(a)$$

holds. After replacing the notion of addition in (2) by that of multiplication, one realises that the multiplication in A is always associative, and that it is commutative if T is a commutative ring. To verify the distributive laws consider :

$$\begin{aligned} \alpha(a)\,[\alpha(b) + \alpha(c)] = \alpha(a)\,\alpha(b+c) = \alpha(ab+ac) &= \alpha(ab) + \alpha(ac) \\ &= \alpha(a)\,\alpha(b) + \alpha(a)\,\alpha(c). \end{aligned}$$

From this formula and the commutative law, the second distributive law follows.

Hence the theorem.

Exercise. Prove : $\alpha(a^n) = \alpha(a)^n$, for any positive interger n, and $\alpha(\mathrm{m}a) = \mathrm{m}\,\alpha(a)$, for any integral number m.

Now $$\alpha(b) + \alpha(-b) = \alpha(0)\,; \qquad \text{hence}$$
$$\alpha(-b) = -\alpha(b), \qquad \text{and therefore}$$
$$\alpha(a-b) = \alpha(a) + (-b) = \alpha(a) - \alpha(b). \qquad \text{Hence}$$

Theorem 2. The necessary and sufficient condition for $\alpha(a) = \alpha(b)$ is $\alpha(a-b) = \alpha(0)$.

The number of the original elements which are mapped on $\alpha(0)$ is important as is seen from the following corollary.

Corollary. Either every element of A is an image of more than one element of a ring T, or every element of A is an image of one and only one element of T.

In the second case A is said to be *isomorphic* to T, and the homomorphism is called an *isomorphism*. An isomorphism is therefore a (1,1)-correspondence of two rings by which the sums, differences and products of corresponding pairs of elements correspond. In some cases therefore isomorphic rings are considered to be equal or to differ by the notation only of the elements, but in general, the notion of isomorphism must be distinguished from that of identity. A ring T may have, *e.g.* two different subrings which are isomorphic. Of special interest is the case when two sets are isomorphic and form the same set; this isomorphism is called an *automorphism*. Hence automorphism is a permutation of elements for which addition and multiplication are invariant. The isomorphism mapping A on B and conversely is sometimes denoted by $A \longleftrightarrow B$.

Examples. 1. The ring of the classes of residues (mod. g) is homomorphic to the ring of the integers.

2. In the ring of the numbers $a + b\sqrt{2}$ (a, b integers), the transformation $a + b\sqrt{2} \rightarrow a - b\sqrt{2}$ is an automorhpism.

2-23. *The ring of classes of residues generated by a homomorphism.* If α is a homomorphism of a ring T, there is a partition of the elements of T into classes, two elements a and b being equivalent if $\alpha(a) = \alpha(b)$, *i.e.*, if $\alpha(a-b) = \alpha(0)$. These classes are classes of residues as considered in 2-13, but they are of a particular kind as the elements c for which $\alpha(c) = (0)$, form a subring T' of T, with the property that each product of an element of T and an element of T' belongs to T'. The converse of this statement is contained in the follwing theorem:

Theorem 1. Let a ring T contain a subring T', and let every product in T, one factor of which is an element of T', be contained in T', then the classes of residues of T' in T form a ring which is homomorphic to T.

Proof. Let $r, r', \ldots$ be elements of T', and let us consider two elements of T to be equivalent if and only if their difference belongs to T'. This definition satisfies the conditions of 2·13, and furnishes therefore a partition of T into classes. Furthermore

$$[\, a + r \,] + [\, b + r' \,] \sim a + b, \text{ and } [\, a + r \,]\, [\, b + r' \,] \sim a\, b.$$

Hence it is admissible to define the addition and the multiplication of the classes $(a), (b), \ldots$ by the corresponding operations exercised on their representatives :

$$(a) + (b) = (a + b), \quad (a)\,(b) = (ab).$$

Every rational formula holding for elements $a, b, \ldots$ remains correct if these elements are replaced in the formula by the classes which they represent. Hence the classes form a module in which the associative law of multiplication and the distributive law hold, *i.e.* they form a ring which is homomorphic to T.

Consider *e.g.* the rings which are homomorphic to the ring R of the integral numbers. To investigate this important class of rings, one has to find out all the subrings of R having the desired property. Every subring is also a submodule ; in the case of R, it is easy to prove that also the converse holds.

Lemma. Every submodule of the ring R of the integral numbers is a ring R_g consisting of the multiples of a non-negative integral number g.

Proof. If $\pm g$ is contained in a submodule M of R, then M contains R_g. Now M either consists of 0 only, and is therefore equal to R_0 or it contains a minimum positive integer, say g. Let m be any number out of M and $m = kg + g'$, where g' is the residue $0 \leqq g' < g$. Then g' is an element of M, and since g is the smallest positive element of M, $g' = 0$. Hence m is contained in R_g, and therefore $M = R_g$.

It is obvious that R_g is a commutative ring, and that it has especially the property, supposed in the preceding theorem, that the product of any element of R and an element of R_g belongs to R_g.

To get the rings which are homomorphic to R, one has to consider the classes of residues of R_g in R (for $g = 0, 1, \ldots$)

Let $g = 0$, then R_0 consists of the number 0 only. Every class of residues consists of one element only. The ring formed by these classes is therefore isomorphic to R.

Let $g = 1$, R_1 is identical with R. There is one class of residues only, all the numbers are equivalent to 0. The ring formed by the classes of residues consists of the nullelement only.

Let $g > 1$. The classes of residues form a commutative ring G consisting of the elements

$$(0), \ldots, (g - 1)$$

which has already been considered in 2-13. G is homomorphic but obviously not isomorphic to R. One has to distinguish whether g is prime, or not. This distinction is afforded by the following two theorems.

Theorem 2. If $g > 1$ is not a prime number, the classes of residues of g form a commutative ring G which is neither itself a field, nor a subring of any field.

Proof. That G is a commutative ring, follows directly from the preceding theorem. As $g > 1$ is not prime, $g = r\,s$, where both the factors are positive and less than g. The classes of residues (r) and (s) are both different from (0), but their product $(r)\,(s) = (0)$. Since in a field the product of two elements which are different from the nullelement, is itself different from the nullelement, G cannot be a field nor a subring of a field.

Theorem 3. The classes of residues

$$(0), (1), \ldots, (p - 1) \tag{1}$$

of a prime number p form a field GF_p.

Proof. To prove the theorem, it must be shown only that for every particular pair of classes $(a) \neq (0)$ and (b), the equation

$$(a)\,(x) = (b) \tag{2}$$

has a sulution. Let (x) run overr the p classes (1), and consider the products (a) (x). If two of them are equal, say $(a)\,(x_1) = (a)\,(x_2)$, then $(a)\,(x_1 - x_2) = (0)$, and therefore $a\,[x_1 - x_2]$ is divisible by p. But since for $(a) \neq (0)$, a is not divisible by p, the factor $x_1 - x_2$ must be divisible by p. Hence $(x_1) = (x_2)$. The p products (a) (x) form therefore p different classes. One of them must be the class (b); the equation (2) has therefore a solution. Hence the theorem.

By this theorem it has been shown that a field may be homomorphic to a ring which is not itself a field. One may wonder whether a ring can be homomorphic to a field; especially it is interesting to know, whether a field can be homomorphic to a field without being isomorphic to it.

Theorem 4. When a ring A which contains more than one element is homomorphic to a field F, then A is isomorphic to F, and A is therefore a field.

Proof. Let $a, b, c, d, \ldots$ denote elements of F. If a and b are represented by the same element of A, then $a - b$ is represented by the nullelement. Let c be represented by an element α of A, which is different from the nullelement, and put $c : (a - b) = d$. The product $d(a - b)$ must be represented by the nullelement, since $a - b$ is represented by it ; this contradicts to the supposition that $d\,(a - b) = c$ is represented by α. Hence any two different elements of F must be represented by different elements of A ; *i.e.* A is isomorphic to F, hence it is a field.

A ring can therefore be homomorphic to a field in the two trivial cases only, where the ring either consists of a nullelement only, or is isomorphic to the field. As a field is supposed to contain more than one element, it follows :

Corollary. If a field is homomorphic to another field, it is isomorphic to it.

2·24. *Subfields of a field.* Let

$$M_1, M_2, \ldots \tag{1}$$

be modules, finite or infinite in number. If these modules have common elements, these form a module, which is called the *meet* of the modules (1), since if a and b are common elements, then $a - b$ belongs to M_1 as well as to $M_2, \ldots$ and is therefore a common element. In the special cases where the modules are rings, the products ab belong also to the meet which is therefore a ring. If the modules are fields, and the meet contains more than one element, the meet itself is a field. A subring F' of a field F which is itself a field, is said to be a *subfield* of F ; this connection is denoted by $F' \subseteq F$ and if $F' \neq F$, by $F' \subset F$. If a subset X of F has the property that the sum, the difference, the product and the quotient of any two elements of X (the divisor being $\neq 0$) belong to X, then X is a subfield of F. Indeed the commutative, associative and distributive laws hold in X as they hold in F. The meet of all the subfields of a field F contains at least the elements 0 and 1, and it is therefore a field which is called the *primefield* of F. The primefield of F is therefore a subfield of F and it is also a subfield of every subfield of F ; the primefield has no other subfield than itself, and it is the only subfield with this property.

Theorem. The elements which one gets by repeated addition, subtraction, multiplication and division of the unitelement of F and of the elements generated in this manner, form the primefield of F.

Proof. Every subfield of F must contain an element different from the nullelement, say the element a. Furthermore it contains $a - a = 0$, $a : a = I$, and it contains all those elements which are generated by repeated addition, subtraction, multiplication and division of I, and of the elements generated successively by these operations. Hence these elements form a set P which is contained in the primefield of F. On the other hand, the sums, differences, products and the quotients—unless the divisor is the nullelement—of two elements of P belong to P. Hence P is a subfield of the primefield and P is therefore the primefield itself.

From this theorem it follows that the primefield of the field of the complex numbers is the field of the rational numbers, and that the fields GF_p are their own primefields.

2·25. *Primefields.* To investigate the primefield of F consider the module generated by the unitelement I of F. This module is a submodule of this primefield, and it consists of the elements

$$n\ I \tag{1}$$

where n takes all the integral numbers. As has been shown in 2-15,

$$pI + qI = (p + q)\ I.$$

To prove the corresponding multiplicative formula

$$[\,pI\,]\,[q\ I\,] = p\,q\cdot I, \tag{2}$$

we use mathematical induction. The formula is obvious for $q = 0$ and every arbitrary integral value of p. From

$$[pI]\ [(q \pm 1)\ I] = [pI]\ \ [qI \pm I] = [pI]\ [qI] \pm pI,$$

it follows that if (2) holds for a particular value of q, then $[pI]\ [(q \pm 1)I] = pqI \pm pI = p\,(q \pm 1)\ I$; thus (2) is correct also for $q + 1$ and $q - 1$. Hence (1) holds for every pair of integral numbers p, q. The module formed by the elements (1) is therefore a ring R^*, and is homomorphic to the ring of the integral numbers. Hence there is no harm in introducing the shorter notation

$$n\ I = n. \tag{3}$$

$p + q$ denotes the element of F which corresponds to $\mathrm{p} + \mathrm{q}$, and it is simultaneously the sum of p and q; the corresponding holds for $p - q$ and $p\,q$. One should notice that the italic characters

$$\mathit{0}, \pm \mathit{1}, \pm \mathit{2}, \ldots, n, \ldots \tag{4}$$

denote elements of F, whereas the roman characters

$$0, \pm 1, \pm 2, \ldots,$$

denote integral numbers which may not be elements of F. On the other hand, the elements (4) may not be different.

Let *e.g.* F be a field GF_{p} [see 2-23, th. 2], say GF_5, then $\mathit{2} = \mathit{7}$, etc. The notation $\mathit{0}$ for the nullelement tallies with the notation of (2-1). The ring of the elements (4) is homomorphic to the ring of the integral numbers, and it is therefore isomorphic to a ring of classes of residues. The null-element corresponds to a subring R_{g} of the ring of the integral numbers [see 22-3]. The number g is called the *characteristic* of the field F.

2-26. *Fields of characteristic p.* Let $\mathrm{g} > 0$. Then R^* is isomorphic to the ring G, as considered in (2-23). From the 2nd theorem of 22-3 it follows that g is a prime number p and R^* is therefore isomorphic to GF_{p}.

Hence R^* is a field, and since R^* is contained in the primefield which has no subfield different from itself, R^* is the primefield of F. Hence :

Theorem. If the characteristic of a field F is different from zero, it is a primenumber p. The primefield consists of the elements

$$\mathit{1}, \mathit{2}, \ldots, p = \mathit{0}$$

and is isomorphic to GF_{p}.

That every primenumber is indeed the characteristic of a suitably chosen field, is obvious by the example of the fields GF_{p}. In a field of a characteristic 2, $a = -a + 2a = -a$ holds ; the positive sign and the negative sign are therefore not different. The calculation in fields of characteristic 2 is much simplified by this fact ; on the other hand there exists no arithmetic mean of two elements. For this reason the case of fields of characteristic 2 has sometimes to be considered separately.

If p is a primenumber, the binomial coefficients

$$\binom{\mathrm{p}}{\mathrm{m}} = \frac{\mathrm{p}\,!}{\mathrm{m}\,!\,(\mathrm{p} - \mathrm{m})\,!}$$

are divisible by p for $0 < m < p$, since the primefactor p does not occur in the denominator. If one calculates in a field of characteristic p, those numbers have therefore to be replaced by zero. Hence in a field of characteristic p

$$(a + b)^p = a^p + b^p \tag{1}$$

holds. Replace b by $-b$, then

$$(a - b)^p = a^p - b^p \tag{2}$$

holds for every odd primenumber p; the same formula holds also for $p = 2$, since in fields of characteristic 2, subtraction is not different from addition. Thus (2) is true for every field of characteristic p.

2·27. *Fields of characteristic* 0. Let $g = 0$; then R^* is isomorphic to R, and therefore it cannot be a field; to find out its nature, apply the following theorem which holds for fields of any characteristic:

Theorem 1. Let A be a subring of a field F, and let A contain more than one element; the meet of those subfields of F which contain A is a field consisting of the solutions X of the equations

$$a\,x = b,$$

where $a \neq 0$ and b are elements of A.

(In other words: The meet of the subfields is proposed to consist of the quotients of the elements of A).

Proof. The meet of those subfields is a field containing the set X of the solutions. One must therefore prove only that X itself is a field. Since A is supposed to contain an element $a \neq 0$, and $a\,1 = a$, $a\,0 = 0$ hold, the elements 0 and 1 belong to X. Therefore X contains more than one element. We need to show only that the sum, the difference, the product and the quotient of any two elements of X (the divisor being supposed $\neq 0$) belong to X. Let $a_1\,x_1 = b_1$, $a_2\,x_2 = b_2$, then

$$a_1\,a_2\,(x_1 \pm x_2) = a_2\,b_1 \pm a_1\,b_2, \tag{1}$$

$$a_1\,a_2\,(x_1\,x_2) = b_1\,b_2, \tag{2}$$

and if $x_1 \neq 0$, and therefore $b_1 \neq 0$:

$$a_1\,b_2\,(x_1 : x_2) = b_1\,a_2. \tag{3}$$

Hence the theorem.

The meet P of all the subfields of F which contain R^* is a subfield of F and contains therefore the primefield; on the other hand, the primefield is one of the subfields of F containing R^*; hence P is the primefield of F. If F is supposed to be of characteristic zero, to every pair of integral numbers r and s $\neq 0$, there corresponds a pair of elements r and $s \neq 0$ in R^* and there exists therefore in P a quotient $r : s$. From (1), (2) and (3) it follows that addition, subtraction, multiplication and division of those quotients are done in the same manner as the corresponding operations for rational numbers. Hence P is homomorphic to the field of the rational numbers. A field cannot be homomorphic to a field, unless the two fields are isomorphic. P is therefore isomorphic to the field of the rational numbers. Hence:

Theorem 2. The primefield of a field of characterisic 0 is isomorphic to the field of the rational numbers.

2·28. *Quotient fields.* The methods used in 2·27, will now be applied to characterise those rings which are *subrings of a field*. As in every field the multiplication is commutative, a ring which is a subring of a field must be a commutative ring; as furthermore the product of two elements which are different from 0, is itself different from 0, the same holds in every subring of a field. It will be shown that these two necessary conditions are also sufficient.

Theorem. Let A be a commutative ring with the property that any pair of its elements which are different from zero, form a product which is different from zero. Then A generates a field which is called the *quotient-field* $Q(A)$ of A. The field $Q(A)$ contains a subring A' which is isomorphic to A and every element of $Q(A)$ is a quotient of two elements of A'.

Proof. Consider the pairs of elements a, b of A for which $b \neq 0$. These pairs are distributed into classes by the help of the following equivalence:

$$a, b \sim a', b'$$

if there exist elements c and d of A such that $c \neq 0$, $d \neq 0$, $ca = da'$ and $cb = db'$. This equivalence is obviously reflexive and symmetric. To prove the transitivity, suppose $a', b' \sim a'', b''$, hence $c'a' = d'a''$, $c'b' = d'b''$, where $c' \neq 0$, $d' \neq 0$. Then $cc'\,a = dd'\,a''$, $cc'\,b = dd'\,b''$. Since $cc' \neq 0$, $dd' \neq 0$, $a, b \sim a'', b''$. Thus the equivalence generates a partition of the pairs into classes. The class represented by a, b will be denoted by a/b. Especially $a/b = ca/cb$. Addition and multiplication of classes will now be defined by the following formulas (well known from the calculation with fractional numbers).

$$a_1/b_1 + a_2/b_2 = (a_1 \, b_2 + a_2 \, b_1)/b_1 \, b_2, \tag{1}$$

$$a_1/b_1 \; a_2/b_2 = a_1 \, a_2/b_1 \, b_2. \tag{2}$$

It must be proved that these formulas are independent of the choice of the representatives.

Let $a_i, b_i \sim a'_i, b'_i,\ \ c_i \, a_i = d_i \, a'_i,\ \ c_i \, b_i = d_i \, b'_i,$ for $i = 1, 2$;

then

$$a_1 \, a_2/b_1 \, b_2 = c_1 \, c_2 \, a_1 \, a_2/c_1 \, c_2 \, b_1 \, b_2 = d_1 \, d_2 \, a'_1 \, a'_2/d_1 \, d_2 \, b'_1 \, b'_2 = a'_1 \, a'_2/b'_1 \, b'_2.$$

Similarly it is shown that

$$(a_1 \, b_2 + a_2 \, b_1)/b_1 \, b_2 = (a'_1 \, b'_2 + a'_1 \, b'_2)/b'_1 \, b'_2.$$

The two commutative laws and the associative law of multiplication are obvious. Now :

$$(a/b + c/d) + e/f = (adf + cbf + bde)/bdf = a/b + (c/d + e/f)$$

(associative law of addition),

$$a/b \;\; c/d + a/b \;\; e/f = ab\,(cf + ed\,)/b^2\,df = a/b\,(c/d + e/f\,) = (c/d + e/f)a/b$$

(distributive laws).

The equation $a/b + x/y = c/d$ is solved by

$$x = cb - ad, \;\; y = b\,d \neq 0\,;$$

the elements a/b form therefore a commutative ring. $0/b$ is its zero-element. For $a \neq 0$,

$$a/b \; u/v = c/d \text{ is solved by } u = bc, \;\; v = a\,d \neq 0.$$

The ring is therefore a field, say $Q(A)$.

For every particular element a of A, there is an element ca/c of $Q(A)$. This element is uniquely determined by a, since

$$ca/c = da/d.$$

As in 2·13, denote this class by (a), then it follows from (1) and (2) that

$$(a) + (b) = (a + b)$$

$$(a) \;\; (b) = (ab).$$

The elements of type (a) form therefore a subring, say A' of $Q(A)$ which is homomorphic to A. If $a \neq b$, then $ca/c \neq cb/c$; hence the homomorphism is an isomorphism. Finally

$$a/b\ (b) = (a).$$

Therefore every element of $Q(A)$ is the quotient of two elements of A'. Hence $Q(A)$ is the quotient field of A, and the theorem holds.

2·29. *Relation between a field and its subrings. Integral domains.* To embed the ring A into a field of which A is a subring, we use the following lemma.

Lemma. Let A be a subring of a ring B, and let A' be a ring which is isomorphic to A; then there exists a ring B' which is isomorphic to B and which contains A' as a subring.

Proof. Denote the elements of A by $\alpha_1, \alpha_2, \ldots$, in general by the letter α with an index but without a dash; the remaining elements of B be denoted by $\beta_1, \beta_2, \ldots$ with indices, but without dash. Consider now an isomorphism J_α mapping A on A' and denote by α'_j the element of A' corresponding to α_j, where j runs over all the indices which occur. If $\alpha_i + \alpha_j = \alpha_k$ and $\alpha_i\ \alpha_j = \alpha_m$, then it follows from the isomorphism that $\alpha'_i + \alpha'_j = \alpha'_k$ and $\alpha'_i\ \alpha'_j = \alpha'_m$. Create now new elements $\beta'_1, \beta'_2, \ldots$ corresponding to the elements $\beta_1, \beta_2, \ldots$ of B. These new elements together with the elements of A', form a set B' which is in a (1,1) corespondence to B; of course the correspondence can be generated by simply affixing a dash on the notations of the elements of B. The addition and the multiplication in B will now be defined in this way. If for any elements ρ, σ, τ and μ of B, $\rho + \sigma = \tau$ and $\rho\sigma = \mu$ hold, then $\rho' + \sigma' = \tau'$, and $\rho'\ \sigma' = \mu'$. By this definition B' is made a ring and the mapping of B on B' generated by affixing a dash becomes an isomorphism J; for the elements of A' this isomorphism is identical with J_α, and the addition and the multiplication of elements of A' is the same as it was defined originally. Hence the ring A' is a subring of B'.

If in particular B is a field, then B' is a field and A' is embedded into B' as a subring. Applying the lemma to the preceeding theorem, one therefore gets the theorem:

Theorem 1. If A is a commutative ring in which 0 cannot be represented as a product of two elements different from 0, then A is a subring of a field which is isomorphic to $Q(A)$.

Definition. A commutative ring containing a unitelement is said to be an *integral domain* if the product of any two of its elements which are both different from zero is itself different from zero.

Hence : An integral domain can be embedded into a field. The close connection between A and its quotientfield $Q(A)$ is shown by the following theorem.

Theorem 2. If A is a subring of F, the meet of all the subfields of F which contain A is isomorphic to $Q(A)$.

Proof. As it has been shown in 2·27 the meet X of those subfields consists of the quotients of the elements of A. Addition, subtraction and multiplication of these quotients are given by the formulas (3), (4) and (5). To every element of $Q(A)$ there corresponds an element of X, and as the formulas (1) and (2) of 2·28 for the rational operations in $Q(A)$ tally with the corresponding formulas of 2·27 for the elements of X, the field X is isomorphic to $Q(A)$. Since $Q(A)$ is a field, the theorem follows from the corollary in 2·23.

2·291. *Identification.* The notion of isomorphism and the lemma of 2·29 can be generalised. Consider any system of mathematical objects which may be subject to certain operations. Modules and rings are instances of such systems ; the objects are called "elements". In a module there is one operation (addition), in a ring there are two operations (addition and multiplication). Another example of a system of this kind is the "affine space" ; its objects are "points" and "vectors" ; the operations are : addition of vectors, multiplication of vectors with real numbers, addition of a point and a vector. A system is therefore not uniquely determined by the objects alone ; of course the same set of objects furnishes different systems if the operations are different. In the same module a "multiplication" can be introduced possibly in more than one way ; thus one may construct two rings which are different, though composed of the same elements. If in the geometrical system just introduced as "affine space", in addition to the operations already introduced, the relation of "scalar product" is established, the affine space becomes a "metric space" which is not the same system as the affine space. Let now Σ and Σ' be any two systems with the same operations, but possibly different elements, and let there be a (1, 1)-correspondence J generated by mapping the elements $\alpha, \beta, \ldots$ of Σ on the elements $\alpha', \beta', \ldots$ of Σ' ; let furthermore R be one of the given operations by which from $\alpha_\nu, \beta_\nu, \ldots$ results $R(\alpha_\nu, \beta_\nu, \ldots, \gamma_\nu) = \kappa_\nu$. If $R(\alpha'_\nu, \beta'_\nu, \ldots, \gamma'_\nu) = \kappa'_\nu$ is the element of Σ' on which κ_ν is mapped by J, then

R is said to be *invariant* for J. If every operation of Σ is invariant, then J is said to be an isomorphism and Σ is isomorphic to Σ'. Obviously the isomorphism satisfies the 3 conditions for an "equivalence". For rings and fields, this general definition of isomorphism tallies with the definitions given earlier. The lemma of 2-28 can be generalised now in the following way:

"Let Σ and T be two systems with the same operations and let every element of Σ be an element of T (*i.e.* Σ is a subsystem of T). If Σ' is isomorphic to Σ, then there exists a system T′ which is isomorphic to T and which contains Σ' as a subsystem".

This lemma is proved in the same way as the lemma in 2-28. The reader may work out the proof as an *exercise.*

Often, isomorphic systems are considered to be equal. They are considered to be different representations of the same thing. *E.g.* one speaks of *the* affine plane though there are different planes which are isomorphic only, but for affine planimetry one needs to consider the common properties of all these planes, and it is therefore convenient to take these planes as representations only of "the" plane. It is not always possible to proceed so; in solid geometry one has to consider simultanously different (isomorphic) planes, say p_1 and p_2, and these may intersect in a line, say s, whereas if p_1 and p_2 are considered to be the same plane, every point of them is a common point; thus one has to distinguish between isomorphic systems in this case. Similarly in Algebra. As far as the properties of a particular ring R are investigated, it is not necessary to make any distinction between R and a ring R' which is isomorphic to R. On the other hand if one discusses a ring S which contains two isomorphic rings R and R', it is necessary to make a distinction between them. There are however cases where two isomorphic systems Σ_1 and Σ_2 will not be considered later on as subsystems of a larger system, *e.g.* when by the introduction of Σ_2, the system Σ_1 becomes superfluous. In this case, there is no harm to *identify* them, *i.e.* to consider them as the representations, or as different names only, of one and the same thing.

Now consider the ring A of the last theorem of 2-28, then its quotientfield $Q(A)$ contains a subring A' isomorphic to A. From the lemma it follows that A can be embedded into a field B which is isomorphic to $Q(A)$; it is now very convenient to identify B with $Q(A)$ and A with A'. Of course, if on building up elementary arithmetic one extends the ring of the integral numbers, at first the quotientfield of the fractions a/b is introduced, and then the fractions $a/1$ are identified with the integral numbers a; otherwise it would be necessary to make a distinction between the fractions a/b and the rational numbers $a{:}b$. That could be done; one is not loosing any logically important step in renouncing identification, but the mathematical language must become very heavy and overloaded by isomorphisms. To understand this clearly, a short review of the steps leading from the notion of natural number to the notion of complex number may be helpful.

(1). Out of the two signs $+$, $-$ and the natural numbers a, form all the pairs $+$ a and $-$ a. These pairs together with a new symbol 0 form a system. Addition and multiplication are defined now in such a manner that the system becomes a ring R and the subsystem of "positive numbers" $+$ a is isomorphic to the system of the natural numbers. Natural numbers are *identified* with positive numbers. R is the ring of *integral numbers.*

(2). Form $Q(R)$ and *identify* R with the subring of the factors with denominator 1. $Q(R)$ is the field of the *rational numbers.*

(3). Form the Dedekind sections in the ordered system of the rational numbers. For a suitable definition of addition and of multiplication, these form a field D. The primefield P of D consists of those sections which are determined by rational numbers. P is *identified* with $Q(R)$, and D is called the field of the *real numbers.*

(4). Form pairs (a, b) of real numbers a, b. For suitably chosen operations of addition and multiplication, these pairs form a field F, and the elements $(a, 0)$ form a subfield which is isomorphic to D. *Identify* D with this subfield. F is the field of the *complex* numbers.

Thus *four* identifications are performed to get the complex numbers starting from the natural numbers. It is well known that there are also different ways; *e.g.* one can define real numbers as continued fractions, or as decimal fractions etc. Similarly complex numbers may be introduced by classes of residues etc. Obviously a Dedekind section is a thing which is different from a continued fraction. The real numbers defined by continued fractions form a field which by its substance is different from the field of the real numbers defined as Dedekind sections; however the two fields are isomorphic. Every mathematical statement holding in one of these fields holds also in the other one. In investigations on mathematical logic, it may be necessary to consider these two fields simultanously, and therefore to make distinction between them. In "pure mathematics" there is no reason to do so; thus we are justified in identifying these two fields (and some others), and to speak of "the" field of the real numbers.

2·3. *Polynomials.*

2·31. *Preliminary investigations.* Let

$$x,\ a_o,\ a_1,\ \ldots,\ a_n,\ b_o,\ b_1,\ \ldots,\ b_m$$

be elements of a ring, then this ring contains also elements

$$a_o + a_1\,x + \ldots + a_n\,x^n = \sum_{o}^{n} a_i\,x^i \tag{1}$$

and

$$b_o + b_1\,x + \ldots + b_m\,x^m = \sum_{o}^{m} b_j\,x^j. \tag{1'}$$

Suppose x to be commutative with every element of the ring. From the laws of addition and multiplication (see 2·1) as far as they are bound to be satisfied in a ring of this kind, it follows that

$$\sum_{o}^{n} a_i\,x^i + \sum_{o}^{m} b_j\,x^j = \sum_{o}^{N} s_\nu\,x^\nu \tag{2}$$

$$\sum_{o}^{n} a_i\,x^i - \sum_{o}^{m} b_j\,x^j = \sum_{o}^{N} d_\nu\,x^\nu \tag{3}$$

$$\sum_{o}^{n} a_i\,x^i \cdot \sum_{o}^{m} b_j\,x^j = \sum_{o}^{M} g_\mu\,x^\mu, \tag{4}$$

where

$$N \geqq n \text{ and } m,\ M \geqq n + m,\ a_{i>n} = 0,\ b_{j>m} = 0,$$

$$s_\nu = a_\nu + b_\nu, \tag{2'}$$

$$d_\nu = a_\nu - b_\nu, \tag{3'}$$

$$g_\nu = \sum_{i+j=\mu} a_i\,b_j. \tag{4'}$$

If ν is greater than n and m, $s_\nu = d_\nu = 0$, similarly for $\mu > n + m$, $g_\mu = 0$. Independently of x, the element (1) of the ring is not altered if some terms with coefficients equal to zero are added. For particular values of x, such expressions may determine the same element, even if they differ in every coefficient, *e.g.* $x - 2$ and $x^2 + 2x - 4$ are equal for $x = 1$. It is of a fundamental importance that there exists a class of rings in which two elements (1) are equal if and only if corresponding coefficients are equal (terms with zero-coefficients being omitted). Every ring can be extended to a ring of this kind by the operation which will be described now.

2-32. *Definition of a polynomial.* For the purpose mentioned above, one starts from a ring R, whose elements are denoted by

$$a_0, a_1, \dots, a_\nu, \dots, b_0, b_1, \dots, b_\mu, \dots, c_0, c_1, \dots, c_\lambda, \dots .$$

Introduce now a symbol x which is not used for the notation of elements of R. Then *create* new elements, the *polynomials in x over R* which are denoted in the same manner as formula (1) of 2-31. It may be emphasised that the polynomials are not yet elements of a ring, but they will be made so by suitable definitions. The system of these polynomials is called

$$R[\,x\,]. \tag{1}$$

As usual, the elements $a_0, a_1, \dots, a_n$ are called *coefficients*, the symbol x is said to be an *indeterminate*. Two polynomials are considered to be *equal* if and only if, after omission of the terms with zero-coefficients, they tally in every coefficient. This definition of equality is admissible, as it satisfies obviously the laws of reflexivity, symmetry and transitivity. For *abbreviation*, we are allowed to omit terms with zero-coefficients, furthermore we may omit any coefficient which is equal to 1 (provided that a unitelement 1 exists in R). Thus the symbol x can itself be considered as a polynomial

$$x = 0 + 1\,x. \tag{2}$$

This formula is not trivial, as — up to now — the sign + in 2-31, (1) is a mere symbol and not the sign of addition. Addition, multiplication and subtraction of polynomials have not yet been defined, but suitable definitions will be given below.

Definition. If $a_i = 0$ for i > d, but $a_d \neq 0$, then d is called the *degree* of the polynomial $\Sigma\, a_i\, x^i$. If every coefficient is zero, the degree is equal to $-$ 1.

By this definition, to every polynomial a definite integral number $\geqq -1$ is alloted as its degree. Equal polynomials have the same degree. The polynomials of degree $-$ 1 are all equal, whereas for degrees $\geqq 0$, there exist different polynomials of the same degree. The polynomials of degree < 1 are of the type

$$a_0 + 0\,x + \dots + 0\,x^n, \tag{3}$$

where a_0 runs over all the elements of R. These polynomials form a subset

$$R^0\,[x] \tag{4}$$

of $R[x]$. Every polynomial (3) is, by the definition of equality of polynomials, equal to a polynomial a_0. Thus there is a (1,1) — correspondence between the elements of the ring R and those of $R^\circ[x]$ so that corresponding elements are written in the same way. The distinction between R and $R^\circ[x]$ will disappear later on.

2-33. *Rings of polynomials.*

Definition. The sum [the product] of two polynomials of $R[x]$ is a polynomial in $R[x]$; the coefficients are determined by (2′) [by (4′)] of 2-31.

Theorem. $R[x]$ is a ring. $R^\circ[x]$ is a subring of $R[x]$ which is isomorphic to R, corresponding elements being denoted in the same way. A polynomial is the sum of one-term polynomials $a_0, a_1x, \ldots, a_nx^n$, and each polynomial a_nx^n is the product of the polynomial a_n (of degree < 1) and the polynomial x^n.

Proof. To show that $R[x]$ is a ring, one has to prove that the commutative law of addition, the associative laws of addition and multiplication, the distributive laws and the law of inverse-existence for addition hold. Since these laws hold in R, one can easily derive them for $R[x]$ by the help of the formulas of 2-31. The commutative law of addition follows directly from (2) and (2′) of 2-31

$$\Sigma\, s_\nu\, x^\nu + \Sigma\, c_\nu\, x^\nu = \Sigma\, t_\nu\, x^\nu,$$

where $t_\nu = s_\nu + c_\nu = a_\nu + b_\nu + c_\nu = a_\nu + (b_\nu + c_\nu)$. Hence $\Sigma\, t_\nu\, x^\nu = \Sigma\, a_\nu\, x^\nu + (\Sigma\, b_\nu\, x^\nu + \Sigma\, c_\nu\, x^\nu)$, *i.e.* the associative law for the addition of polynomials. Similarly one shows that $(\Sigma\, a_\nu\, x^\nu\ \Sigma\, b_\nu\, x^\nu)\ \Sigma\, c_\nu\, x^\nu$ and $\Sigma\, a_\nu\, x^\nu(\Sigma\, b_\nu\, x^\nu\ \Sigma\, c_\nu\, x^\nu)$ are both equal to $\Sigma\, u_\nu\, x^\nu$, where $u_\nu = \sum\limits_{\nu=\kappa+\lambda+\mu} a_\kappa\, b_\lambda\, c_\mu$. It may be left to the reader, to check the two distributive laws in the same manner. If d_ν is defined by 2-31, (3′), $\Sigma\, d_\nu\, x^\nu + \Sigma\, b_\nu\, x^\nu = \Sigma\, a_\nu\, x^\nu$ follows from (2′) of 2-31. Hence $R[x]$ is a ring. The remaining propositions of the theorem are immediate consequences of the definition of addition and multiplication of polynomials.

Since $R^\circ[x]$ is isomorphic to the ring R, one *identifies* the elements of $R^\circ[x]$ with the elements of R which are already denoted in the same manner. It is therefore not necessary any more to distinguish between the polynomial a_0 (of degree < 1) and the element a_0 of R. The ring $R[x]$ is an *extension* of the ring R since by the identification carried out just before, R becomes a subring of $R[x]$. As every subring (and even every submodule) of a ring (a module) contains the nullelement of the ring (module), the rings $R[x]$

and R have the same nullelement. *I.e.* the nullelement 0 of R is also the nullelement of $R[x]$. Furthermore if R contains a unitelement 1, this unitelement is also the unitelement of $R[x]$.

Since a polynomial has been proved to be the sum of its terms (which are polynomials with at most one coefficient different from zero), one can interchange the terms without altering the polynomial, *e.g.* one can write the terms in the opposite order

$$a_n\, x^n + a_{n-1}\, x^{n-1} + \dots + a_0.$$

Exercises. Let R be a ring which may or may not be commutative but contains a unitelement.

1. Prove that x^n is commutative with every polynomial of $R[x]$.

2. Let $R[x]$ be a subring of a ring R_1, prove that $R[x]$ is the meet of all those subrings of R_1 which contain R and x.

2-34. *Commutative rings of polynomials.*

Theorem 1. If R is a commutative ring, then $R[x]$ is a commutative ring.

Proof. By the theorem of 2-33, it has been shown that $R[x]$ is a ring; one has only to check the commutativity of the multiplication. Of course the commutativity follows from 2-31, (4′) and $\sum\limits_{i+j=m} a_i\, b_j = \sum\limits_{i+j=m} b_i\, a_j$.

Theorem 2. If R is an integral domain, so is $R[x]$.

Proof. As in consequence of theorem 1, $R[x]$ is a commutative ring containing the unitelement 1, one has to prove only that if $\sum\limits_0^n a_\nu\, x^\nu$ and $\sum\limits_0^m b_\nu\, x^\nu$ are of degree $\geqq 0$, then the same holds for there product $\sum\limits_0^{n+m} g_\mu\, x^\mu$. Without loss of generality we can suppose that $a_n \neq 0$ and $b_m \neq 0$, hence $g_{n+m} = a_n\, b_m \neq 0$. Hence the theorem.

In a similar way one proves:

Theorem 3. If R is a subring of a field, then the degree of the product of two polynomials of $R[x]$ is the sum of the degrees of the factors, provided the factors are both of degree $\geqq 0$.

Exercise. Show that the condition: "R is an integral domain" cannot be replaced in theorem 2 by: "R is a commutative ring".

Theorem 4. $R[x]$ is not a field.

Proof. If R consists of the nullelement only, then $R[x]$ is equal to R, and as it consists of one element only, it is not a field. Let $a \neq 0$ be an element of R, then $R[x]$ contains $a\,x$. If $R[x]$ is a field, R is a subring of a field; hence theorem 3 can be applied. On the other hand there exists in $R[x]$ a polynomial of degree, say m, which is inverse to ax. The product of the two polynomials is equal to 1, and therefore it is a polynomial of degree 0. Now $m > -1$, but from the theorem 3 it follows that $m + 1 = 0$. This is a contradiction.

2-35. *Integral functions.* Let C be a commutative ring containing the unitelement 1; then the same holds for $C[x]$. Let $a_0, a_1, \ldots, a_n$ be elements of C, and λ an arbitrary element of $C[x]$, then

$$a_0 + a_1\,\lambda + a_2\,\lambda^2 + \ldots + a_n\,\lambda^n = f(\lambda) \tag{1}$$

is again an element of $C[x]$. The correspondence mapping λ on $f(\lambda)$ is called an *integral rational function over C* or briefly (as we are only concerned with Algebra) an *integral function* over C. These functions map the elements of C on elements of C, and the elements of $C[x]$ on elements of $C[x]$. Especially 0 is mapped on a_0, and x (which indeed is an element of $C[x]$ as 1 is supposed to be an element of C) is mapped on the polynomial $f(x)$ which has the same coefficients as (1) has. On the other hand, given any polynomial in x over C, there exists an integral function over C having the same coefficients; one has only to replace the indeterminate x by the *variable* λ running over the elements of $C[x]$ or a subset of them.

Again consider all the polynomials in x over C, say

$$f(x),\ \ f_1(x),\ f_2(x),\ \ldots$$

and any particular element of $C[x]$, say λ. To every element $f(x)$ of C let correspond the element $f(\lambda)$ which also belongs to $C[x]$. Let $f_1(x)$ and $f_2(x)$ be any two elements of $C[x]$

$$f_1(x) = \Sigma\, a_i\, x^i,\ \ f_2(x) = \Sigma\, b_j\, x^j,\ \ f_1(x) + f_2(x) = f_3(x) = \Sigma\, s_\nu\, x^\nu,$$
$$f_1(x)\, f_2(x) = f_4(x) = \Sigma\, g_\mu\, x^\mu.$$

Then the coefficients a_i, b_j, s_ν, g_μ are interconnected by 2-31, (2′) and (4′).

Since $C[x]$ is a commutative ring, λ is commutative with the elements a_i and b_j. Hence (see 2-31) the addition and the multiplication of $\Sigma\, a_i\, \lambda^i$ and $\Sigma\, b_j\, \lambda^j$ is done also in accordance with 2-31, (2), (2′), (4) and (4′). Therefore

$$f_1(\lambda) + f_2(\lambda) = f_3(\lambda), \quad f_1(\lambda)\, f_2(\lambda) = f_4(\lambda) \text{ hold.}$$

The correspondence $f(x) \to f(\lambda)$ is therefore a homomorphism. By it, the ring of all the elements of $C[x]$ is mapped on a subring C_λ which is homomorphic to $C[x]$.

Let $\lambda = b$ be an element of C. Then every element of C_b is an element of C; on the other hand the polynomials $x + (a - b)$ of $C[x]$ are mapped on a, which is supposed to be an arbitrary element of C. Hence $C_b = C$. Thus every element of C generates an homomorphism mapping $C[x]$ on C.

Exercises: Consider the homomorphism generated by an element λ of $C[x]$: (1) if λ is of degree > 1, (2) if λ is of degree 1 and C is a field.

By an homomorphism the nullelement is always mapped on the nullelement. If therefore

$$F(f_1(x), \ldots, f_n(x)) = 0,$$

then

$$F(f_1(\lambda), \ldots, f_n(\lambda)) = 0$$

for every λ out of $C[x]$. Hence

Theorem. Every equation between elements of $C[x]$ remains correct if for x one puts any particular element of $C[x]$.

It may be mentioned that the commutativity of C is essential for the validity of this theorem.

2-36. *Polynomials in two indeterminates. Derivatives.* Let R be a ring, x and y be indeterminates, then

$$R[x] = T, \quad R[y] = S$$

are also rings. $T[y]$ consists of the polynomials in y of which the coefficients are polynomials in x over R, *i.e.* it consists of the sums

$$\Sigma\, a_{jk}\, x^j\, y^k, \tag{1}$$

where a_{jk} runs over the elements of R. The same holds for $S[x]$. Hence

$$T[y] = (R[x])\,[y] = S[x] = R[x,y]. \tag{2}$$

This statement can easily be generalised for any number of indeterminates.

Thus we can *extend* R to

$$R[x_1, x_2, \ldots, x_n]$$

without making any distinction about the order in which the extension is performed.

Let

$$\varphi(x) = \Sigma\, a_j\, x^j, \text{ and } \Sigma\, \varphi(0) = 0, \text{ then } a_0 = 0 \text{ and } \varphi(x) = x\, \varphi_1(x),$$

where $\varphi_1(x)$ is a polynomial in x over the same ring as $\varphi(x)$ is, provided this ring contains a unitelement.

Let D be an integral domain; as in 2-25 the sum of n terms, each being equal to 1, is denoted by n. Now let $f(x)$ be a polynomial of $D[x] = T$, then $f(x + y)$ is a polynomial of $T[y]$.

$$f(x + y) - f(x) = F(y), \;\; F(0) = 0.$$

Hence

$$F(y) = y\, F_1(y).$$

Now $F_1(0)$ is an element of $T = D[x]$, say

$$F_1(0) = f'(x), \tag{3}$$

where $f'(x)$ is a polynomial in x over D and is uniquely determined by $f(x)$. The polynomial $f'(x)$ is said to be the *derivative* of $f(x)$. If D consists of real numbers only, this notation tallies with what in Analysis is called the derivative of an integral rational function. The reader knows that in Analysis the notion of derivative applies to a much larger class of functions of a real variable than rational functions only. Here, a derivative is defined for polynomials only, but the coefficients are not necessarily real numbers. The formulas for the derivatives of sums and products are the same as in Analysis even the proofs are nearly the same, the only consideration being that there is no passage to limit. Readers are advised to compare carefully the following proofs with those given in analysis to understand clearly the difference between an indeterminate and a variable which takes real values some of them making the functions possibly senseless.

Let

$$f(x) = f_1(x) + f_2(x),$$

then

$$\begin{aligned} y\, F_1(y) &= \{ f_1(x + y) - f_1(x)\} + \{ f_2(x + y) - f_2(x)\} \\ &= y\{F_{11}(y) + F_{21}(y)\}. \end{aligned}$$

Hence

$$y\{F_1(y) - F_{11}(y) - F_{21}(y)\} = 0.$$

Since D and therefore $D[y]$ are integral domains, and y is not the nullelement of $D\,[y]$, the factor in brackets is zero. Put $y = 0$ then from (3) follows :

$$f'(x) = f'_1(x) + f'_2(x). \tag{4}$$

Similarly, let

$$g(x) = f_1(x)\, f_2(x),$$

then

$$\begin{aligned} y\, G_1(x) &= \{ f_1(x+y) - f_1(x)\}\; f_2(x+y) + \{ f_2(x+y) - f_2(x)\}\, f_1(x) \\ &= y\{F_{11}(y)\; f_2(x+y) + F_{21}(y)\, f_1(x)\}, \end{aligned}$$

wherefrom it follows by the same consideration as above that

$$g'(x) = f'_1(x)\, f_2(x) + f'_2(x)\, f_1(x). \tag{5}$$

Furthermore :

$$f'(x) = 0 \qquad \text{for } f(x) = c$$

$$f'(x) = 1 \qquad \text{for } f(x) = x. \tag{6}$$

From (4), (5), (6) it follows in the same way, as in analysis :

For

$$f(x) = \Sigma\, a_j\, x^j, \;\; f'(x) = \Sigma\, \mathrm{j}\, a_j\, x^{j-1}. \tag{7}$$

2·37. *Homogeneous polynomials.* Again let D be an integral domain; $x_1, \ldots, x_n, t$ be indeterminates, denote

$$D_1 = D[x_2, \ldots, x_n],\, D_2 = D[x_1, x_3, \ldots, x_n], \ldots, D_n = D[x_1, \ldots, x_{n-1}] \tag{1}$$

hence

$$S = D[x_1, \ldots, x_n] = D_k\,[x_k], \text{ for } k = 1, \ldots, n. \tag{2}$$

Every polynomial $f(x_1, \ldots, x_n)$ of S can be considered to be a polynomial in x_k over D_k

$$f(x_1, \ldots, x_n) = \; f_k(x_k), \;\; k = 1, \ldots, n. \tag{3}$$

Consider now the polynomial

$$f(tx_1, \ldots, tx_n)$$

which belongs to $S[t]$.

Definition. $f(x_1, \ldots, x_n)$ is said to be *homogeneous of degree m* if

$$f(tx_1, \ldots, tx_n) = t^m\, f(x_1, \ldots, x_m) \tag{4}$$

holds.

Let $f(x_1, \ldots, x_n)$ be homogeneous of degree m. Put

$$f(x_1, \ldots, x_n) = \Sigma\, a_j\, x_1^{\nu_{1j}}, \ldots, x_n^{\nu_{nj}}, \tag{5}$$

where to different j correspond different sets $(s_j, \dots, w_j)$. Then $t^m f(x_1, \dots, x_n) = f(tx_1, \dots, tx_n) = \Sigma\, a_j\, x_1^{s_j}, \dots, x_n^{w_j}\, t^{s_j + \dots + w_j}$.

Hence
$$s_j + .. + w_j = m, \text{ for every occuring } j \tag{6}$$

is a necessary condition for $f(x_1, \dots, x_n)$ to be homogeneous of degree m. Obviously this condition is also sufficient. Forming the n derivatives and multiplying each of them with the corresponding indefinite x_k, one gets

$$x_1\, f'_1(x_1) = \Sigma\, s_j\, a_j\, x_1^{s_j} \dots x_n^{w_j}$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$x_n\, f'_n(x_n) = \Sigma\, w_j\, a_j\, x_1^{s_j} \dots x_n^{w_j},$$

where, as in 2-25, (3), s_j stands for the element which one gets by taking the unitelement s_j times. By addition it follows from (6) that

$$\sum_{k=1}^{n} x_k\, f'_k(x) = m\ f(x_1, \dots, x_n) \tag{7}$$

holds. (*Euler's formula*).

2·4. *Factorisation.*

Fundamental notions. Suppose R to be a commutative ring. If a, b, c are elements of R, and

$$a\, b = c \tag{1}$$

holds, a and b are said to be *factors* of c, and c is said to be *divisible by* a and b. Whereas in a field every element is divisible by every element different from zero, there is no corresponding theorem for rings. As some rings — *e.g.* the ring of the integral numbers, and the rings $R[x]$ — play an important role in mathematics, it is necessary to consider the mutual divisibility of elements of certain classes of rings which are not fields.

Let D be an integral domain. If every element of D is divisible in D by a particular element say e, then 1 is divisible by e, and therefore e^{-1} belongs to D. If on the other hand, e and e^{-1} belong to D, then for every a of D, the elements $a\, e^{-1}$ and ae belong to D; hence every element a of D is divisible by e and e^{-1}. Thus the elements which are factors of every element of D are exactly those elements of which an inverse element exists in D. The unitelement 1, for instance, has this property; so these elements are called the *unities* of D. If e_1 and e_2 are unities, then the same holds for $e_1\, e_2$ and $e_1\, e_2^{-1}$. *Thus the unities in D form a multiplicative commutative group.*

Some examples : 1. Let D be the ring of the integral numbers, then $+1$ and -1 are the only unities.

2. Let F be a field, then every element different from zero is a unity.

3. The unities of $F[x]$ are the polynomials of degree 0 (*i.e.* the elements of F, with exception of 0).

Let a and b be two elements of D for which $a : b = e$ is a unity of D; then a and b are said to be *associated*. This association of elements satisfies the laws of reflexivity, symmetry and transitivity ; thus D is partitioned into *classes* of associated elements (*associates*).

Every element of D is divisible by its associates and by the unities. A non-zero and non-unity element which is not divisible by any other element than its associates and unities, is said to be a *prime-element*. *E.g.* in the ring of the integral numbers, an element is associated to itself and to its negative ; the primenumbers taken with positive or negative sign are the prime-elements. In an arbitrary field the non-zero elements are all unities, but there might be elements which are neither zero nor unities and are non-divisible by any prime-element provided the domain D is suitably chosen. *E.g.* consider the numbers

$$a_0 + a_1 2^{\frac{1}{2}} + a_2 2^{\frac{1}{4}} + \dots + a_n 2^{2^{-n}}, \tag{2}$$

for $n = 0, 1, \dots$ and $a_0, a_1, \dots$ being integral numbers. The numbers (2) form an integral domain D with the unities 1 and -1, the prime-elements being the odd primenumbers with positive or negative sign. The number *2* is not a unity and is not divisible by any prime-element of D.

If an element can be represented as a product of unities and prime-elements it is said to be *factorisable* ; the representation itself is called a *factorisation*. Obviously a prime-element is always factorisable. If an element a is non-factorisable, it is neither a unity nor a prime, and it is divisible by an element b which is not associated to a and is itself non-factorisable. Two factorisations of an element will not be considered to be different if there is a (1, 1)-correspondence between the prime-elements, corresponding prime-elements being associated. If all the factorisations of an element a are equal in this sense, then the factorisation of a is said to be *unique*. If the factorisation of every element which is neither zero nor a unity is unique, then one says that *the factorisation in D is unique*. Thus the factoristion in a field is unique.

Exercises. (1) Construct an integral domain D which is not a field but has no prime-element.

(2) Investigate the extension of the notions explained here to rings which are not integral domains.

2·42. *Domains with factorisable elements.*

Theorem. Let D be an integral domain and to every element $a \neq 0$ of D let there correspond an integral positive number $N(a)$, the *norm*, such that

$$N(ab) \geqq N(a), \tag{1}$$

where equality holds if and only if b is a unity, then every element $\neq 0$ in D is factorisable.

Proof. If a is a product of non-unity elements,

$$a = a_1 \ldots a_m$$

then

$$N(a) \geqq N(a_1 \ldots a_{m-1}) + 1 \geqq N(a_1 \ldots a_{m-2}) + 2 \ldots \geqq m. \tag{2}$$

Again, if a is not factorisable, it is the product of two non-unities, say $a = a_1 b_1$ of which at least one, say b_1, is not factorisable. Hence

$$a = a_1 b_1 = a_1 a_2 b_2 = \ldots a_1 a_2 \ldots a_n b_n,$$

where n can be chosen $> N(a)$ and none of the factors is a unity. But from (2), $N(a) \geqq$ n $+ 1$ which is a contradiction. Hence the theorem.

Examples. (1) Let D be the domain of the integral numbers, and $N(a)$ be the absolute value: $N(a) = |a|$. Then $N(a)$ satisfies (1). Hence the integral numbers are factorisable.

(2) Let D be the set of the numbers

$$\alpha + \beta\sqrt{(-6)}, \tag{3}$$

where α, β take all the integral values; then D is an integral domain.

Put

$$N(\alpha + \beta\sqrt{(-6)}) = \alpha^2 + 6\beta^2 = (\alpha + \beta\sqrt{(-6)})(\alpha - \beta\sqrt{(-6)}), \tag{4}$$

then

$$N(ab) = N(a)\,N(b) \tag{5}$$

and for $a \neq 0$, $N(a) > 0$ is an integral number.

If $N(\alpha + \beta\sqrt{(-6)}) = 1$, then $(\alpha - \beta\sqrt{(-6)}) = 1 : (\alpha + \beta\sqrt{(-6)})$; hence $\alpha + \beta\sqrt{(-6)}$ is a unity. Therefore

$N(ab) = N(a)\,N(b) > N(a)$ if b is not a unity. On the other hand, if e is a unity,

$$1 = N(1) = N(e\,e^{-1}) = N(e)\,N(e^{-1}),$$

and therefore $N(e) = 1$ as 1 has no positive factor other than 1. Finally $N(ae) = N(a)\ N(e) = N(a)$. Hence the norm (4) satisfies the condition (1). In this integral domain the factorisation is not unique, since

$$6 = 2 \cdot 3 = -[\sqrt{(-6)}]^2.$$

We have to prove that 2, 3 and $\sqrt{(-6)}$ are prime-elements in D. $N(2) = 4$, $N(3) = 9$, $N(\sqrt{(-6)}) = 6$. If one of the 3 elements would not be prime, there must be elements of which the norm is equal to 2 or 3. If α is an integral number

$$\alpha^2 \equiv 0, \text{ or } 1 \pmod{3} \tag{6}$$

according as α is divisible by 3 or not. Again let $N(\alpha + \beta\sqrt{(-6)}) = 2$, then $\alpha^2 + 6\beta^2 = 2$, $\alpha^2 \equiv 2 (\text{mod. } 3)$ contrary to (6). Let $N(\alpha + \beta\sqrt{(-6)}) = 3$, then $\alpha^2 + 6\beta^2 = 3$, therefore α is divisible by 3, say $\alpha = 3\kappa$ multiplying with $2 : 3$ one gets $6\kappa^2 + 4\beta^2 = 2$, hence $(2\beta^2) \equiv 2$ (mod. 3) contrary to (6). Thus 2, 3 and $\sqrt{(-6)}$ are prime-elements ; so 6 can be factorised in two different ways.

2·43. *Unique factorisation*. The following criterion is often used.

Criterion for uniqueness of factorisation. Let D be an integral domain in which every element $\neq 0$ is factorisable. The necessary and sufficient condition for the uniqueness of the factorisation is that no product ab can be divisible by a prime-element p, unless a factor a or b is divisible by p.

Proof. (1) Let the factorisation be unique in D. One gets the factorisation of $c = a\,b$ by putting together the factorisation of a and that of b. On the other hand $c = d\,p$, and one gets the factorisation of c, by putting together the factorisation of d and the prime-element p. From the uniqueness of the factorisation it follows that an associate of p occurs among the prime-factors of a or of b. Hence a or b is divisible by p.

(2) Let the above condition for the products hold ; then it can be proved by mathematical induction that if $a\,a_1 \ldots a_n$ is divisible by p, at least one of the factors is divisible by p. Of course the proposition holds for $n = 1$; suppose it to be true for $n < m$. If $a\,(a_1 \ldots a_m)$ is divisible by p, and a is not divisible by p, the product in brackets is divisible by p, and therefore one of the factors is divisible by p. Let now c be factorised $c = p_1 \ldots p_n$, and c be divisible by a prime-element p, then at least one of the prime-elements p_i is divisible by p and therefore associated with p. Suppose now, there exist in D elements which are not uniquely factorisable, and let r be the minimum number of prime-factors (which are not necessarily

all different) such that $b = q_1 \dots q_r$ admits a different factorisation $b = p_1 \cdots p_s$ (where s = or ≠ r). Obviously r > 1. As b is divisible by p_s, one of the factors q_j is associated with $p_s = u\, q_r$, where u is a unity. Then $q_1 \cdots q_{r-1} = p_1 \cdots p_{s-1} u$ are different factorisations, contrary to the supposition that products of less than r prime-elements are uniquely factorisable. Hence the theorem.

If to two elements a and b of D there exists in D a common factor

$$(a,\ b) \tag{1}$$

such that every common factor of a and b is a factor of (a, b), then (a, b) is called a *highest common factor*, or *h. c. f.* of a and b. Every element of D associated to $(a,\ b)$ is also an *h. c. f.* of a and b. Conversely two *h. c. f.* of a and b must, by definition, be divisible one by the other and are therefore associated. Hence (1) is not determined uniquely, but up to a unity-factor only, provided that an *h. c. f.* exists at all.

Suppose that to every pair of elements of D there exists an *h. c. f.*, then every common factor of 3 elements, say a, b, c, is a common factor of $(a,\ b)$ and c, and therefore a factor of $d = ((a,\ b),\ c)$. On the other hand, d is a common factor of a, b and c. Thus there exists an *h. c. f.* to every triplet of elements of D. Obviously this *h. c. f.* is uniquely determined up to a unity-factor. By repeating the procedure, the following result is easily obtained :

Theorem 1. If to every pair of elements of D an *h. c. f.* exists, then there exists to every n-tuplet $a_1, \dots, a_n$ of elements of D an *h. c. f.*

$$(a_1, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n) \tag{2}$$

which is uniquely determined up-to a unity-factor. An element of D is a common factor of the elements of the n-tuplet if and only if it is a factor of (2).

The operation for *h. c. f.* is commutative and associative ; moreover it satisfies a distributive law :

$$a\,(b,\ c) = (a\,b,\ a\,c). \tag{3}$$

Let D be uniquely factorisable, and

$$a = p_1^{r_1}\, p_2^{r_2} \dots p_m^{r_m}, \tag{4}$$

where $p_1, p_2, \dots, p_m$ are different prime-elements. If $0 \leqq s_j \leqq r$ for $j = 1, \dots, m$, then for every unity e,

$$e \; p_1^{s_1} \ldots p_m^{s_m} \tag{5}$$

is a factor of a. On the other hand, it follows from the above criterion that a and therefore any factor of a can be divisible by such prime-elements only, as are associated to $p_1, \ldots, p_m$. As $p_2^{r_2} \ldots p_m^{r_m}$ is not divisible by p_1, the element a and any factor of a cannot be divisible by $p_1^{r > r_1}$. Similarly for the other prime-elements. Hence the elements (5) are the only factors of (4). Given two elements a and b of D. Using the notation $p^{0}_{j} = I$, one can express both elements simultaneously by

$$a = p_1^{r_1} \ldots p_m^{r_m}, \quad b = u \; p_1^{t_1} \ldots p_m^{t_m}, \text{ where } u \text{ is a unity.} \tag{6}$$

An element (5) is therefore a common factor of a and b, if $0 \leqq s_j \leqq r_j$ and $s_j \leqq t_j$ hold for $j = 1, \ldots, m$. Let w_j be the smaller of the two numbers r_j and t_j, then

$$(a, \; b) = p_1^{w_1} \ldots p_m^{w_m} \tag{7}$$

is an *h. c. f.* of a and b. Hence

Theorem 2. If in D the factorisation is unique, there exists a highest common factor for every pair of elements $\neq 0$.

These considerations on unique factorisation tally nearly verbatim with the corresponding theory of elementary arithmetic. The only essential difference consists of the unities which occur as factors and which remain arbitrary to a certain extent. In the domain of the integral numbers, there exist two unities $+1$ and -1 and therefore the prime-elements occur in pairs of associated ones, but in arithmetic, one uses to give preference to the positive numbers, thus the factorisation becomes unique in a stricter sense. In the general case considered here, there is no way of making a similar distinction.

2·44. *Euclidean domains.* Let c_1, c_2 run over the elements of D, and a, b be two particular elements; then the elements

$$c_1 \; a + c_2 \; b \tag{1}$$

form a commutative ring which with every element contains also its multiples and especially its associates. Every element (1) is divisible by every common factor of a and b. If the *h. c. f.* $(a, \; b)$ is an element of the form (1), then the set of the elements (1) consists exactly of those elements which are divisible by $(a, \; b)$. This case is of a special interest.

Theorem 1. If the elements $\neq 0$ of D are factorisable, and for every pair a, b of elements of D, an *h. c. f.* exists, and can be expressed by (1), then D is uniquely factorisable.

Proof. Let ab be divisible by a prime-element p, say $ab = k\,p$, and a not be divisible by p, then the highest common factors of a and p are unities; hence a unity, say e^{-1} can be expressed by $c\,a + d\,p = e^{-1}$. Hence $(c\,e)\,(a\,b) + (d\,e\,b)\,p = b = (c\,e\,k + d\,e\,b)\,p$. Therefore b is divisible by p. Hence the theorem follows from the criterion of 2·43.

Let

$$a_1, a_2, \ldots, a_n, a_{n+1} \tag{2}$$

be elements of the integral domain D satisfying the following conditions

$$\begin{aligned} a_1 \;\; &+ b_2\,a_2 = a_3 \\ a_2 \;\; &+ b_3\,a_3 = a_4 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{k-1} &+ b_k\,a_k = a_{k+1} \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n-1} &+ b_n\,a_n = a_{n+1}. \end{aligned} \tag{3}$$

Then every common factor of a_{k-1} and a_k is also a common factor of a_k and a_{k+1}, and conversely, and since this property holds for every k, each pair of consecutive elements has the same common factors. If especially $a_{n+1} = 0$, then a_n is the *h. c. f.* of a_n and a_{n-1}, therefore every pair of consecutive elements of the sequence (2) has an *h. c. f.* and this factor is equal to a_n. Hence

$$a_n = (a_1, a_2). \tag{4}$$

The construction of a sequence (2) ending with $a_{n+1} = 0$ is called the "Algorithmus of the *h. c. f.*". This algorithmus allows one to express successively $a_3, a_4, \ldots, a_n = (a_1, a_2)$ as linear homogeneous functions of a_1 and a_2. If therefore the elements $\neq 0$ of D are factorisable, and the algorithmus can be performed for every pair of elements, then D is uniquely factorisable. Thus it is very important to have a condition which is sufficient for the working of the algorithmus. Let in an integral domain D a norm-function N be determined which satisfies the conditions explained in 2·42. Let furthermore to every pair of elements $a_{k-1} \neq 0$ and $a_k \neq 0$ of D exist elements a_{k+1} and b_k of D such that

$$a_{k-1} + b_k\,a_k = a_{k+1}, \tag{5}$$

$$\text{where either } a_{k+1} = 0, \text{ or } N(a_{k+1}) < N(a_k),$$

then D is said to be a *Euclidean domain*.

Theorem 2. To every m-tuplet of elements of a Euclidean domain D, there exists in D an *h. c. f.* which can be found out by a repeated application of the algorithmus; the *h. c. f.* can be represented as a linear homogeneous function of the n elements with coefficients out of D. The factorisation in D is unique.

Proof. Since a norm-function exists in D, the elements are factorisable. From (5) it follows, that given any two elements a_1 and a_2, one can find a sequence $a_2, a_3, \dots$, in D such that $N(a_2) > N(a_3) > \dots$. As the norms are positive integers, their sequence cannot have more than $N(a_2)$ elements. If $N(a_n)$ is the last norm in the sequence, it follows from (5) that $a_{n+1} = 0$. Hence $a_n = (a_1, a_2)$ can be found out by the algorithmus, and therefore $a_n = ba_1 + ca_2$, where b and c are elements of D. The theorem holds therefore for m = 2, and the factorisation in D is unique. From 2·43, theorem 1 it follows that the *h. c. f.* of every m-tuplet exists. Suppose that

$$(d_1, \dots, d_k) = b_1 d_1 + \dots + b_k d_k,$$

and that this *h. c. f.* can be found out by applying the algorithmus k − 1 times, then

$$\begin{aligned}(d_1, \dots, d_{k+1}) = ((d_1, \dots, d_k), d_{k+1}) &= d(b_1 d_1 + \dots + b_k d_k) + c_{k+1} d_{k+1} \\ &= c_1 d_1 + \dots + c_{k+1} d_{k+1}\end{aligned}$$

can be found out by applying the algorithmus k times. Hence the theorem.

2·45. *The domain of the integral numbers.* Consider the domain J of the integral numbers, and put

$$N(a) = |a|.$$

This function has obviously the properties postulated for a norm-function in 2·42, (1), and it satisfies also the condition 2·44, (5). Hence the factorisation in J is unique, and the *h. c. f.* can be found by the algorithmus. The multiplicative properties of integral numbers are therefore determined by their representation as products of powers of primenumbers. Thus it is important to know that *there exists an infinite number of primenumbers.*

Proof (*Euclid*). Suppose there exists a finite number of primenumbers only, say the numbers p_j ($j = 1, \ldots, n$); then $(p_1\ p_2 \ldots p_n) + 1$ is neither divisible by any primenumber, nor is it a unity. Hence the supposition is wrong, and the above proposition holds.

2-46. *Homomorphism modulo a prime-element.* Suppose D to be an integral domain, where factorisation is unique, and let p be any particular prime-element in D. The elements which are divisible by p form a subring D_p of D. As has been shown in 2-23, the classes of residues of D_p in D form a ring D^p which is homomorphic to D. By this homomorphism an element a of D is mapped on an element (a) of D^p. Hence $(a) = (a + k\,p)$ for every element k of D. The zero-element (0) of D^p consists of the elements divisible by p, i.e. the elements of D_p. Since D is commutative, and D^p is homomorphic to D, the ring D_p is commutative. It will be shown now that *D^p is an integral domain.* Suppose $(a)\,(b) = (0)$, then $(a\,b) = (0)$, that means that $a\,b$ is divisible by p. Since the factorisation in D is supposed to be unique, and p is a prime-element, at least one of the factors a, b must be divisible by p, i.e. one of the elements (a), (b) of D must be the zero-element. Furthermore (1) is the unitelement of D^p. Hence the commutative ring D^p is an integral domain.

2-47. *Factorisation in $F\,[x]$.* Consider now the domain $F\,[x]$ of the polynomials in x over a field F (see 2-34); with exception of the element 0, for every element $f(x)$ of $F\,(x)$ a positive integral *norm* is defined by

$$N\,(\,f\,(x)\,) = degree\,(\,f\,(x)\,) + 1. \tag{1}$$

The elements $\neq 0$ of F are the unities. Hence $N(a) = 1$ holds for unities only. Applying 2-34, theorem 3, one gets for non-zero-elements a, b of $F[x]$

$$N(a\,b) = N(a) + N(b) - 1. \tag{2}$$

Hence $N(a\,b) \geqq N(a)$, where equality holds if and only if b is a unity.

Let

$$f_1(x) = \sum_1^n a_\nu\,x^\nu,\ f_2(x) = \sum_1^m b_\mu\,x^\mu,\ \mathrm{n} \geqq \mathrm{m},\ b_m \neq 0$$

be two polynomials of $F\,[x]$. The condition $\mathrm{n} \geqq \mathrm{m}$ does not involve any loss of generality, as e.g. a_n may be equal to zero; the condition $b_m \neq 0$ only forbids $f_2(x)$ to be the zero-element.

$$f_1(x) - (a_n : b_m)\, x^{n-m}\, f_2(x) = \sum_{0}^{n-1} a^1{}_r\, x^r = \phi_1(x)$$

. . . .

$$\phi_k(x) - (a^k{}_{n-k} : b_m)\, x^{n-m-k} f_2(x) = \sum_{0}^{n-k-1} a^{k+1}{}_r\, x^r = \phi_{k+1}(x)$$

. . . .

$$\phi_{n-m}(x) - (a^{n-m}{}_m : b_m)\ f_2(x) = \sum_{0}^{m-1} a^{n-m+1}{}_r\, x^r = f_3(x)$$

then
$$f_1(x) + b_2(x)\, f_2(x) = f_3(x), \tag{3}$$
where the degree of $f_3(x)$ is less than the degree of $f_2(x)$.

Hence

$$\text{either} \quad N\,(\,f_3(x)\,) < N\,(\,f_2(x)\,) \tag{4}$$
$$\text{or} \quad f_3(x) = 0. \qquad \text{Hence}$$

Theorem 1. Let $f_1(x)$ and $f_2(x) \neq 0$ be polynomials of $F\,[x]$ (where F denotes a field), then there exist in $F\,[x]$ polynomials $b_2\,(x)$ and $f_3\,(x)$ satisfying (3) and (4), and these polynomials can be calculated by a finite number of steps.

The method of calculating $b_2\,(x)$ and $f_3\,(x)$ is called the *algorithmus of division* and $f_3\,(x)$ is the *remainder*. By theorem 1 it is established that the norm-function satisfies the conditions of 2-44. Hence :

Theorem 2. $F\,[x]$ is a Euclidean domain ; the *h. c. f.* of any m elements $\phi_1, \ldots, \phi_m$ can be represented as a linear homogeneous function $g_1(x)\ \phi_1(x) + \ldots + g_m(x)\ \phi_m(x)$, and the factorisation is unique.

It may be mentioned that $f_3(x)$ is uniquely determined by (3) and (4), since if $f_1(x) + c\,(x)\ f_2(x) = \psi\,(x)$, $f_3\,(x) - \psi\,(x)$ is divisible by $f_2\,(x)$, and $\psi\,(x)$ therefore cannot satisfy the conditions stated for $f_3(x)$ in (4), unless $\psi\,(x) = f_3\,(x)$ holds. A similar uniqueness does not hold in the domain J of the integral numbers. Indeed

$$12 - 7 = 5 \qquad \text{N}(5) = 5 < \text{N}(7) = 7.$$
$$12 - 2.7 = -2 \qquad \text{N}(-2) = 2 < \text{N}(7) = 7.$$

The prime-elements of $F[x]$ are said to be *irreducible polynomials*. Since polynomials of degree zero are unities, an irreducible polynomial of degree $\geqq 1$ cannot be represented as a product of two polynomials of degree $\geqq 1$.

Hence every linear polynomial in x over F is irreducible. A polynomial of degree $\geqq 1$ which is not irreducible is said to be *reducible*. If F is a subfield of F_1, every polynomial $f(x)$ of $F[x]$ belongs also to $F_1[x]$; $f(x)$ may be irreducible in $F[x]$ and reducible in $F_1[x]$. E.g. the polynomial $f(x) = x^2 - 2$ is a polynomial of $F[x]$, where F is the field of the rational numbers; in $F[x]$, the polynomial $f(x)$ is irreducible. Let F_1 be the field of the real numbers, then $f(x) = (x - \sqrt{2})(x + \sqrt{2})$ is reducible in $F_1[x]$.

Theorem 3. Let $f_1(x)$ and $f_2(x)$ be two polynomials of $F[x]$, and let there be no common irreducible factor of $f_1(x)$ and $f_2(x)$, then there exist polynomials $\phi_1(x)$ and $\phi_2(x)$ of $F[x]$ such that

$$\phi_1(x)\, f_1(x) + \phi_2(x)\, f_2(x) = 1 \tag{5}$$

holds.

Proof. Every highest common factor of $f_1(x)$ and $f_2(x)$ is a unity of $F(x)$, i.e. any element $a \neq 0$ of F. From theorem 1 it follows that there exist polynomials $\psi_1(x)$ and $\psi_2(x)$ satisfying $\psi_1(x)\, f_1(x) + \psi_2(x)\, f_2(x) = a$. Putting $\psi_i(x) = a\, \phi_i(x)$ (for i = 1, 2), one gets (5).

If especially $f_2(x)$ is irreducible, and $f_1(x)$ is not divisible by $f_2(x)$, then $\phi_1(x)\, f_1(x) \equiv 1$ (mod. $f_2(x)$), i.e.

$$\phi_1(x) \equiv \{ f_1(x) \}^{-1} \ (\mathrm{mod}\ f_2(x)\,). \tag{6}$$

In 2-46 it has been shown that in an integral domain with unique factorisation, the classes of residues of a prime-element form an integral domain. As $F[x]$ is an integral domain with unique factorisation, the classes of residues of $f(x)$ form an integral domain, and as (6) holds, these classes form a field. Hence:

Theorem 4. Let $f(x)$ be irreducible in $F(x)$, then the classes of residues of $f(x)$ in $F[x]$ form a field.

If $f(x)$ is reducible, say $f(x) = \phi(x)\, \psi(x)$, then the classes of residues do not form an integral domain since $f(x)$ is not a prime-element. Of course between the classes, the equation $(\phi(x))\,(\psi(x)) = (f(x)) = (0)$ holds, though $(\phi(x)) \neq (0)$ and $(\psi(x)) \neq (0)$.

The elements of the field considered in the last theorem are classes of residues of $f(x)$. Let n be the degree of $f(x)$ and let $f_1(x)$ be any polynomial of $F[x]$, then one gets by the algorithmus of division

$$f_1(x) - b(x)\, f(x) = f_2(x),$$

where $f_3(x)$ is the remainder of the division and therefore of a degree $< n$. Since $f_1(x) - f_3(x)$ is divisible by $f(x)$, $f_3(x)$ belongs to the same class of residues as $f_1(x)$; thus every class contains a polynomial of degree $< n$. Let there be two such polynomials, say $f_3(x)$ and $f_4(x)$ in the same class, then $f_3(x) - f_4(x)$ is of degree $< n$ and divisible by $f(x)$, hence it is zero. Thus in every class there exists one and only one polynomial of degree $< n$ which characterises the class. Consider in particular the classes containing polynomials a_0 of degree < 1. These classes form a subfield which is in a (1, 1) and isomorphic correspondence with the elements a_0 of F. This subfield is therefore isomorphic to F. Hence:

Theorem 5. Each of the classes of residues as considered in theorem 4 contains exactly one polynomial of a degree which is less than the degree of $f(x)$, and characterises the class. The classes characterised by polynomials of degree < 1 (i.e. elements of F) form a subfield which is isomorphic to the field F, every class being represented by its characterising element.

2·48. *Factorisation in* $D[x]$. Let D be an integral domain with unique factorisation; consider the factorisation in $D[x]$. At first the divisibility of polynomials $f(x)$ of $D[x]$ by elements of D will be investigated. In the special case where D is a field, every $f(x)$ is divisible by every element of D which is different from zero as these elements are unities. This special case has been investigated already in 2·47.

If $f(x)$ is divisible by an element c of D, then

$$f(x) = c \sum b_\nu x^\nu = \sum cb_\nu x^\nu; \tag{1}$$

hence every coefficients of $f(x)$ is divisible by c. If the *h. c. f.* of the coefficients of $f(x)$ is equal to 1, then $f(x)$ is divisible by unities only, and conversely. In this case $f(x)$ is said to be a *primitive* polynomial of $D[x]$.

Let p be any prime-element of D; as in 2·46, the subring of the elements which are divisible by p will be denoted by D_p.

Then $D_p[x]$ consists of the polynomials the coefficients of which are divisible by p, whereas $\{D[x]\}_p$ consists of the polynomials of $D[x]$ which are divisible by p. From (1) it follows that

$$D_p[x] = \{D[x]\}_p. \tag{2}$$

As the factorisation in D is unique, the classes of residues of D_p in D form an integral domain D^p of which D_p is the zero-element (see 2·46); from 2·34, theorem 2 it follows that $D^p[x]$ also is an integral domain of which the class $D_p[x]$ is the zero-element. The classes of residues of $\{D[x]\}_p$ in $D[x]$ form a ring $\{D[x]\}^p$ which is isomorphic to $D^p[x]$ and is therefore an integral domain. Let $\phi(x) = f_1(x) f_2(x)$ be divisible by p, then $\phi(x)$ belongs to the zero-element $\{D[x]\}_p$ of $\{D[x]\}^p$ and therefore at least one of the two factors is divisible by p. Hence:

Lemma. If the factorisation in D is unique and p is a prime-element of D, furthermore $f_1(x)$ and $f_2(x)$ belong to $D[x]$ and $f_1(x) f_2(x)$ is divisible by p, then at least one of the factors $f_1(x)$ and $f_2(x)$ is divisible by p.

Corollary 1. If $f_1(x)$ and $f_2(x)$ are primitive polynomials, then $f_1(x) f_2(x)$ is primitive.

Corollary 2. If $a\phi(x)$ is divisible by a primitive polynomial $f(x)$, then $\phi(x)$ is divisible by $f(x)$.

Proof. Since a belongs to D, it is factorisable ; $a = p_1 p_2 \cdots p_n$. Let

$$a\,\phi(x) = f(x)\, f_1(x).$$

Since $f(x)$ is primitive, it is not divisible by p_1 ; hence from theorem 1 it follows that $f_1(x) = p_1 f_2(x)$, and therefore

$$p_2 \cdots p_n\, \phi(x) = f(x)\, f_2(x).$$

By n—fold repetition of the procedure, one gets

$$\phi(x) = f(x)\; f'_{n+1}(x).$$

Corollary 3. If $f(x)$ is factorisable in $D[x]$, then $f(x) = a_1 \dots a_m$ $f_1(x) \dots f_n(x)$, where $f_1(x), \dots, f_n(x)$ are primitive, and $a_1 \dots a_m = a$ is the factorisation in D of the *h. c. f.* of the coefficients of $f(x)$.

Proof. A prime-element of $D[x]$ is either an element of D, or it is a primitive polynomial since if the coefficients have a common non-unity factor, a polynomial is not a prime-element. Let $f_1(x), \dots, f_n(x)$ be the primitive polynomials of degree > 0 among the prime-factors of $f(x)$, then the product of them is a primitive polynomial, say $\phi(x)$. The product of the prime-factors of $f(x)$, belonging to D is an element a of D. Thus $f(x) = a\,\phi(x)$. Hence a is the *h.c.f.* of the coefficients of $f(x)$. The factors a_ν of a are prime in $D[x]$, hence they are also prime-elements of D and $a = a_1 \dots a_m$ is a factorisation of a in D.

Theorem. If the factorisation in D is unique, so the factorisation in $D[x]$ is.

Proof. Since D is an integral domain, there exists a quotient-field F, of which D is a subring; every element of F is the quotient of two elements of D. Let $f(x)$ be a primitive polynomial of $D[x]$, then $f[x]$ is also a polynomial of $F[x]$, and it is uniquely factorisable in $F[x]$

$$f(x) = \varphi_1(x) \dots \varphi_n(x).$$

The factors $\phi_i(x)$ are determined up to a unity of $F[x]$, i.e. up to an element of F. Since the coefficients of $\varphi_i(x)$ are quotients of elements of D, there exists an element $b_i \neq 0$ such that $b_i\, \varphi_i(x)$ is a polynomial in $D[x]$, hence

$$b_i\, \varphi_i(x) = c_i\, f_i(x),$$

where $f_i(x)$ is primitive. $f_i(x)$ and $\varphi_i(x)$ are associated in $F[x]$, hence $f_i(x)$ is a prime-element of $F[x]$, moreover $f_i(x)$ is a prime-element in $D[x]$, otherwise it must be a product of primitive polynomials in $D[x]$, contrary to the fact that it is a prime-element of $F[x]$. Putting $b_1 \dots b_n = b$, $c_1 \dots c_n = c$, one gets

$$b\, f(x) = c\, f_1(x) \dots f_n(x).$$

From the corollaries 1 and 2 it follows that the primitive polynomials $f(x)$ and $f_1(x) \dots f_2(x)$ are divisible one by the other one and are therefore associated. Hence

$$f(x) = e\, f_1(x) \dots f_n(x),$$

where e is a unity, and $f_1(x), \dots, f_n(x)$ are prime-elements of $F[x]$ as well as of $D[x]$. In the special case where $f(x)$ is a prime-element of $D[x]$, the number n is equal to 1. Every prime-element of $D[x]$ which does not belong to D is therefore also a prime-element of $F[x]$. Since the factorisation of $f(x)$ in $F[x]$ is unique, the primitive polynomial $f(x)$ is factorisable in $D[x]$ into prime-elements $f_i(x)$ of $D[x]$ which are determined up to unities of $F[x]$ i.e. up to elements of F. But since each $f_i(x)$ is primitive, these elements must be unities of D. Hence $f(x)$ is uniquely factorisable into the prime-factors of a and those of $f_i(x)$, $(i = 1, \dots, n)$ these factorisations being unique. On the other hand it follows from Corollary 3 that every factorisation of $a\, f(x)$ consists of a factorisation of a and a factorisation of $f(x)$. Hence the theorem.

This theorem may be considered as a generalisation of 2·47, theorem 1, but it does not generalise its full statement. Of course $D[x]$ is not necessarily a Euclidean domain, even if D is. Consider e.g. the domain J of the integral numbers which has been proved to be a Euclidean domain. $a(x) = x - 2$ and $b(x) = x + 2$ are primitive polynomials of $J[x]$ and are of degree 1 ; hence they are prime-elements. Since ± 1 are the only unities, they are non-associated ; hence $(a(x), b(x)) = 1$. If this *h.c.f.* would be linearly dependent on $a(x)$ and $b(x)$, say

$$u(x)\ a(x) + v(x)\ b(x) = 1,$$

then this equation must hold when x is replaced by any element of J ; for $x = 0$, one gets $-2\,u(0) + 2\,v(0)$ which is obviously even and therefore $\neq 1$. Hence $J[x]$ is non-Euclidean.

Exercise. Let $a(x)$ and $b(x)$ be two polynomials of $E[x]$, where E is a Euclidean domain ; show that $f(x) = a(x)\ u(x) + b(x)\ v(x)$ if and only if $f(x)$ is divisible by a particular polynomial.

2-49. *Comparison between R and R* $[x]$. If the factorisation in D is unique, then the same holds for

$$D_1 = D[x_1],\ D_2 = D_1[x_2],\ \ldots,\ D_n = D_{n-1}[x_n] = D[x_1, \ldots, x_n].$$

Hence the polynomials in n variables form a uniquely factorisable domain if the coefficients run over a uniquely factorisable ring, e.g. a field, of the domain J of the integral numbers. On the other hand starting from a domain of this kind, one gets again integral domains by a homomorphism which maps a particular prime-element and its multiples on zero.

In 2-3 and 2-4, two methods have been developed to generate new rings, integral domains and fields from given ones ; these two procedures are of a fundamental importance for general algebra. One method consists of the construction of a ring of polynomials over a given ring, the other is a homomorphism by which a suitable subring is mapped on zero. The following collection of results obtained before may be useful.

Let R be	then R $[x]$ is	see
a ring	a ring	2-33, th.1
a commutative ring	a commutative ring	2-34, th.1
an integral domain	an integral domain	2-34, th.2
uniquely factorisable	uniquely factorisable	2-42
a field	not a field, but a Euclidean domain	2-34, th.4 2-47, th.2.

Moreover: If in D the factorisation is unique and D_p is the subring of the elements which are divisible by a particular prime-element p, then D is mapped on an integral domain D^p by the homomorphism mapping D_p on zero [see 2-46]. It is not necessary that D^p has a unique factorisation.

If in particular $D = F[x]$, where F is a field, then D^p is a field. (see 2-47, th. 4).

2-5. *The fundamental theorem of General Algebra.*

2-51. *Existence of a root in a suitable extension.* Let α be any element of a field F, and $f(x)$ be a polynomial of the ring $F[x]$. From the algorithmus of division, one gets

$$f(x) = (x - \alpha)\ \phi(x) + \beta,$$

where $\phi(x)$ is a polynomial of $F[x]$ and β is an element of F. By putting $x = \alpha$, (see 2-35) one gets $f(x) = \beta$; hence

$$f(x) = (x - \alpha)\ \phi(x) + f(\alpha). \tag{1}$$

Therefore $f(x)$ is divisible by $(x - \alpha)$ if and only if $f(\alpha) = 0$. If in particular $f(x)$ is an irreducible polynomial of a degree > 1, it cannot be divisible by any factor of degree 1, and therefore there is no element α in F which satisfies the equation

$$f(\alpha) = 0. \tag{2}$$

To solve the equation (2), it is therefore necessary to consider a field F_1 of which F is a subfield. Every polynomial $f(x)$ of $F[x]$ is also a polynomial of $F_1[x]$, but if $f(x)$ is an irreducible polynomial of $F[x]$, nevertheless it may be a reducible polynomial of $F_1[x]$; in particular $f(x)$ may be divisible by a factor $x - \alpha$, where α is an element of F_1. In this case, α satisfies the equation (2). If F is a subfield of F_1, then F_1 is called an *extension* of F, and if α satisfies the equation (2), then α is said to be a *root* of the polynomial $f(x)$. To find a root of an irreducible polynomial $f(x)$ of $F[x]$, one has to extend F to a field F_1 which contains such an element α that $f(x) = (x - \alpha)\ f_1(x)$, where $f_1(x)$ is a polynomial of $F_1[x]$. Let e.g. F be the field of the rational numbers; then $f(x) = x^2 - 2$ is irreducible, but $f(x)$ is also a polynomial of $F_1[x]$ when F_1 is the field of the real numbers. As a polynomial of $F_1[x]$, $f(x) = (x - \sqrt{2})\ (x + \sqrt{2})$ is reducible. Let F_2 be the field of the complex numbers, then $x^2 + 1$ which is an irreducible polynomial of $F_1[x]$ is a reducible polynomial of $F_2[x]$. A fundamental question of general algebra is whether, given a polynomial $f(x)$

of $F[x]$, one can always extend F to F_1 in such a way that $f(x)$ has a root in F_1. This question is answered in the affirmative by the following theorem.

Fundamental theorem of General Algebra. If $f(x)$ is a polynomial of $F[x]$, then there exists an extension F_1 of F which contains a root α of of $f(x)$.

Proof. Since $f(x)$ is a product of (one or more) irreducible polynomials, and the roots of these polynomials are also roots of $f(x)$, there is no loss of generality to suppose that $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ is irreducible. The classes of residues of $F[x]$ modulo $f(x)$ form a field F'_1, and the classes characterised by elements a of F form a subfield which is isomorphic to F. By this isomorphism the class $a_0 + k(x) f(x)$ corresponds to the element a_0 of F (see 2·47, th. 5). One can therefore extend the field F to a field F_1 which is isomorphic to F'_1. Let α be the element of F_1 which corresponds to the polynomial x, then $a_0 + a_1 \alpha + \ldots + a_n \alpha^n$ corresponds to the class containing the polynomial $a_0 + a_1 x + \ldots + a_n x^n = f(x)$, but this class is the class (0). Hence $f(\alpha) = 0$ and α is a root of $f(x)$.

2·52. *Extensions of F containing a root of $f(x)$.* Let $f(x)$ be a polynomial of degree n which is irreducible in $F[x]$. Again consider the field F_1 which is isomorphic to the field of the classes of residues of $f(x)$ in $F[x]$. By $\phi_r(x)$, polynomials of $F[x]$ of a degree $< n$ will be denoted; then every class of residues of $f(x)$ contains one and only one element of the type $\phi_r(x)$ and the elements of F_1 can therefore be represented by

$$\phi_r(\alpha) = b^r_0 + b^r_1 \alpha + \ldots + b^r_{n-1} \alpha^{n-1}. \tag{1}$$

Different polynomials $\phi_{r'}(x)$ belong to different classes of residues and correspond therefore to different elements of F_1. Hence every element of F_1 can be represented in one and only one manner by (1) and it corresponds (1, 1) to the ordered set

$$b_0, b_1, \ldots, b_{n-1} \tag{2}$$

of elements of F. Those elements for which $b_1 = \ldots = b_{n-1} = 0$, correspond to the elements of F. To add (subtract) two elements of F_1, one has to add (subtract) the corresponding coefficients (2). The addition and the subtraction is therefore performed as if the elements were *vectors*; the corresponding holds for multiplication with elements of F.

Let now $\phi_1(\alpha)$ and $\phi_2(\alpha)$ be any pair of elements of F_1. From 2-47, theorem 1 it follows that by the algorithmus of division, a polynomial $\phi_3(x)$ satisfying

$$\phi_1(x)\,\phi_2(x) - k(x)\,f(x) = \phi_3(x) \tag{3}$$

can be found; hence

$$\phi_1(\alpha)\,\phi_2(\alpha) = \phi_3(\alpha) \tag{4}$$

can be obtained by a calculation composed of a finite number of elementary operations in the field F. Let $\phi_1(\alpha) \neq 0$, then $\phi_1(x) \neq 0$. As $f(x)$ is a primitive element of the ring $F[x]$, and therefore relatively prime to $\phi_1(x)$, the highest common factor $(f(x), \phi_1(x)) = 1$ can be obtained by the algorithmus of the *h.c.f.* Hence a polynomial $\phi_4(x)$ of degree $< n$ satisfying

$$\phi_1(x)\,\phi_4(x) + h(x)\,f(x) = 1 \tag{5}$$

can be found by elementary operations in F, and

$$1 : \phi_1(\alpha) = \phi_4(\alpha). \tag{6}$$

The considerations leading to the fundamental theorem enable us therefore to extend the field F to a field F_1 which contains a root of $f(x)$ and in which the elementary operations (addition, subtraction, multiplication, division) can be performed by methods based only on the elementary operations in F. Thus if F is *given* in the sense that one can perform the elementary operations in every case by a finite number of steps, the same holds for F_1. On the other hand F_1 is not uniquely determined, but in the sense of isomorphism only. Obviously there are extensions of F which contain a root of $f(x)$ and are non-isomorphic to F_1, e.g. every extension of F_1 has that property. It will be shown now that every extension of F which contains a root, say α of $f(x)$ contains a subfield which is an extension of F, and is isomorphic to F_1.

Theorem. Let $f(x)$ be an irreducible polynomial of $F[x]$, and E be any extension of F which contains any root, say α of $f(x)$; then the meet of all the subfields of E which contain F and α, form a field which is isomorphic to the field F'_1 of the classes of residues of $f(x)$ in $F[x]$.

Proof. Every subfield of E, which contains F and α, contains also the elements

$$\phi(\alpha) = b_0 + b_1\,\alpha + \dots + b_{n-1}\,\alpha^{n-1}, \tag{7}$$

where n is supposed to be the degree of $f(x)$, and the coefficients run independently over all the elements of F, and $\phi(x)$ again denotes a polynomial of degree $< n$. Obviously the elements (7) form a module M. Let $\phi_1(\alpha)$, $\phi_2(\alpha)$ be two elements of M ; if $\phi_3(x)$ is determined by (3), then $\phi_3(\alpha) = \phi_1(\alpha)\, \phi_2(\alpha)$. Hence M is a ring which is homomorphic to the field F'_1. As has been proved in 2-23, the module M is a field and is isomorphic to F'_1. On the other hand, every subfield of E containing F and α must contain M, thus it is the meet of all the subfields of E which contain M. Hence the theorem.

2-53. *Factorisation of $f(x)$ into linear factors. General remarks.* It has been shown in 2-52 that the fundamental theorem of general algebra is far more than a mere theorem on existence of roots. Fields in which those roots exist, can actually be constructed, and the operations of addition, subtraction, multiplication and division can be performed practically in the extended field. By the last theorem it has been shown that if the polynomial $f(x)$ under consideration is irreducible in $F(x)$, there exists one extension F_1 of F which is uniquely determined in the sense of isomorphism, such that every extension of F containing a root of $f(x)$ is isomorphic to an extension of F_1. Obviously there exists an infinite number of extensions of F which are isomorphic to F_1; one can even arrange them in such a way that they have no common elements other than elements of F. In each of these fields there exist roots of $f(x)$. It is therefore of no use to speak of *the* roots of $f(x)$, but only of the roots of $f(x)$ *in a particular field*. About the number of roots of a polynomial of degree n in a field, the following theorem holds :

Theorem. Suppose $f(x)$ to be a polynomial in $F[x]$ of degree n.
1. If F' is any extension of F, then $f(x)$ has not more than n roots in F'.
2. There exists an extension, say F^* of F, such that in F, $f(x) = a(x - \alpha_1) \dots (x - \alpha_n)$, where a belongs to F^*, and $\alpha_1, \dots, \alpha_n$ belong to F, and this representation of $f(x)$ in $F^*[x]$ is unique up to an arbitrary permutation of $\alpha_1, \dots, \alpha_n$.

Proof. 1. Let $\alpha_1, \dots, \alpha_m$ be roots of $f(x)$ in F'. Then $f(x)$ is divisible by $x - \alpha_j$ where $j = 1, \dots, m$; since the factorisation in $F'[x]$ is unique, $f(x)$ is divisible by $(x - \alpha_1) \dots (x - \alpha_m)$ which is a polynomial of degree m. Hence $m \leqslant n$.

2. If $n = 1$, then the proposition holds for $F^* = F$. Suppose by mathematical induction, that the proposition holds for degrees $< m$, and let $n = m$. From the fundamental theorem it follows that F has an ex-

tension F_1 which contains a root, say α_m, then $f(x)$ is divisible in $F_1[x]$ by $x - \alpha_m$, say $f(x) = f_1(x)(x - \alpha_m)$. Now $f_1(x)$ is of degree $m - 1$, and from the supposition made for mathematical induction, it follows that $f_1(x) = a(x - \alpha_1)\dots(x - \alpha_{m-1})$, and therefore $f(x) = a(x - \alpha_1)\dots(x - \alpha_m)$. The uniqueness of the representation follows from the uniqueness of the factorisation of $f(x)$ in $F^*[x]$. Hence the proposition follows by mathematical induction.

By this theorem it is shown that the number of the roots of a polynomial does not exceed the degree in any field and that it is equal to the degree (certain roots possibly being counted multiply) in a suitably chosen extension. It is however often of a great interest to know the exact number of the roots in a particular field, e.g. in the field of the real numbers or in the field of the complex numbers. These problems are not solved by the fundamental theorem of general algebra, they need investigations of a special kind. For the field of the complex numbers, the question is completely solved by the "fundamental theorem of classical algebra". Methods of determining the number of the real solutions of any polynomial with real coefficients will be given in 5·2. The fundamental theorem of general algebra and other theorems derived from it are of a more general nature than the classical investigations on real and complex roots. In the general theory one does not suppose that the coefficients of the polynomial are numbers; they may be elements of any field, e.g. they may be polynomials in an indeterminate y with complex coefficients

$$f_0(y) + f_1(y)x + \dots + f_n(y)x^n = F(x, y). \tag{1}$$

Thus it follows from the fundamental theorem of general algebra, that a suitable extension of the quotientfield of the polynomials $f(y)$ contains an element α, for which $F(x, y) = 0$. This consideration is the very basis of the theory of algebraic functions. On the other hand, it is obvious that the field of the real numbers and the field of the complex numbers are of a special interest as they play an important role in nearly every branch of mathematics. Thus the classical question for the roots of a polynomial in these fields is of general importance far beyond its historical interest. In enquiring about the roots in the field of the real (the complex) numbers, one is in general not satisfied to know the number of the roots in the intervals (the domains) of the real axis (the complex plane). By choosing these intervals (domains) suitably small, one gets approximately values of the roots. To determine the "magnitude" of a root, means nothing else than to construct a way leading to an approximation of the root with an error less than any predetermined number. Of course, an irrational number cannot be determined otherwise than by a method approximating it by rational numbers. Even the most familiar formulas expressing irrational numbers (e.g. $\sqrt{2}$) are only rules for an approximation given in a short form. The importance of an approximative calculation of the roots is obvious, especially for problems of applied mathematics. On the other hand, if the elements of a field are not put into a definite order, there are no intervals or domains in that field. For this reason, the question about the magnitude of a root, does not arise at all in general algebra.

Thus the problem "to solve an algebraic equation" needs for itself some more detailed specification. If one wants to find a root in any *suitable* extension, then one has to apply only the methods of 2·52. Again, if the roots in any *particular* field are required (e.g. the field of the real numbers, or of the complex numbers), then methods appropriate to the special nature of that field are necessary. For the field of the complex numbers, the "fundamental theorem of classical algebra" (see 3·8) gives the most important information. Sometimes, the problem is put also in a different way. "Is there a root of the given polynomial in a *suitable* field out of a *particular* class of fields ?" To this class of problems belongs the investigation of those roots which can be expressed by a finite number of radicals (square roots, cubic roots, etc.). Again an interesting special case concerns those roots which can be expressed by a successive drawing of square roots; every problem of planimetry which can be solved by the help of ruler and compass leads to a root of this class.

2·6. *Extension of a field.*

2·61. *Vectorspaces over a field.* The representation of the extension F_1 of F as performed in 2·52 reminds one of the vectorspaces considered in Chapter I; this similarity has already been mentioned in 2·52. The only essential difference is, that the coordinates are elements of F which is supposed to be an arbitrary field, whereas in Chapter I, the coordinates have been supposed to be numbers. It has been mentioned on *p.* 26 that—except for 1·7—the property of the coordinates "to be numbers" can be disposed of easily. Thus a more general definition of a vectorspace will be given now. Let M be a module, and F be a field; the elements of F are denoted by characters $a, b, c, \ldots$ and the elements of M by Greek characters $\alpha, \beta, \delta, \ldots$ The common nullelement of M and of F is denoted by 0. Suppose that the elements of M can be multiplied by the elements of F, the products being elements of M, and that for this multiplication, the following laws hold :

$$\begin{aligned} a(b\alpha) &= (ab)\alpha \\ a(\alpha+\beta) &= a\alpha + a\beta \\ (a+b)\alpha &= a\alpha + b\alpha \\ 1\,\alpha &= \alpha. \end{aligned} \tag{1}$$

Then M is said to be a *module over F*. Now

$0\,\alpha = (c - c)\alpha = c\alpha - c\alpha = 0$. Similarly it follows from (1) that $c\,0 = 0$, whether the factor 0 in $c0$ is regarded as the zero-element of F or of M.

Let in particular M be a module over F, where there exists a *basis* of n elements of M

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

such that every element α of M can be represented by

$$\alpha = a_1\,\alpha_1 + \ldots + a_n\,\alpha_n, \tag{2}$$

and that

$$c_1\,\alpha_1 + \ldots + c_n\,\alpha_n = 0 \text{ implies } c_1 = \ldots = c_n = 0\,; \tag{3}$$

then M is a *vectorspace over F of rank* n, and the elements of M are called *vectors*. If

$$\alpha = a_1\,\alpha_1 + \ldots + a_n\,\alpha_n = b_1\,\alpha_1 + \ldots + b_n\,\alpha_n,$$

then

$$0 = (a_1 - b_1)\,\alpha_1 + \ldots + (a_n - b_n)\,\alpha_n,$$

hence it follows from (3), that $a_1 - b_1 = \ldots = a_n - b_n = 0$. The representation of a vector of M by (2) is therefore unique. Thus there exists a (1,1)-mapping of the vectors of M on the ordered sets of n elements of F

$$(a_1, \ldots, a_n) \tag{4}$$

the addition of vectors and the multiplication of vectors and elements of F being determined by

$$\begin{aligned} (a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 + b_1, \ldots, a_n + b_n) \\ c\,(a_1, \ldots, a_n) &= (ca_1, \ldots, ca_n). \end{aligned} \tag{5}$$

Hence :

Theorem. Every vectorspace of rank n over F is isomorphic to the system of all the ordered n-tuplets (4), where the operations of addition of vectors and of multiplication of a vector with an element of F are determined by (5).

In particular, a "vectorspace W of rank n over the field of the real (or the complex) numbers" is *isomorphic* to the "vectorspace V of rank n" of Chapter I. Every vector of W is *represented* by an n-vector $(x_1, \ldots, x_n)$ of V. But W is *not identical* with V, nor are the vectors of W identical with the n-vectors which represent them, as the latter ones are n-tuplets by definition. Of course, if a different basis of W is used, the vectors of W are mapped in a different way on the n-vectors of V. In consequence of the isomorphism between W and V, the formulas established for V can be applied to W, and it is often convenient to identify V and W. On the other hand, whenever different representations of the same vector will be considered (e.g. in 6-2) it is necessary to distinguish between a vector of W and its representation by an n-vector of V. In a corresponding manner the notion of n-vector will be used in connection with vectorspaces over any field K.

A *linear transformation of a vectorspace W over* K is a mapping of W on itself leaving invariant addition of vectors and their multiplication with elements of K. This definition tallies with a characteristic property of linear transformations of spaces V of n-vectors [see 1-(11), th. 2]. Thus $\xi \to \xi'_i$ implies $\Sigma c_i \xi_i \to \Sigma c_i \xi'_i$ when $c_1, \ldots, c_m$ are elements of K. In the same way as theorem 2 of 1-(11) has been proved, one shows easily that the n-vectors $(x_1, \ldots, x_n)$ representing the vectors of W are transformed by linear equations

$$x'_i = \Sigma a^i_k x_k \tag{6}$$

with coefficients a^i_k out of K, when W is transformed by a linear transformation. On the other hand, every transformation (6) corresponds to a linear transformation of W when any basis of W is selected.

2-62. *Extension of the results of Chapter* I *to vectorspaces over an arbitrary field.* If F is the field of the real (or the complex) numbers, a vectorspace over F is isomorphic to a vectorspace as considered in Chapter I of this book. It was however a matter of convenience only that in Ch. I the coordinates of a vector have been supposed to be numbers. With the only exception of 1-7, no other property of "numbers" has been used than that they form a field. For this reason it was stated in 1-16 that the notion of number could be understood as real number or as complex number. The reader may check that 1-2 to 6, and 1-8 to 11 hold without any further alteration if the notion of "number" is systematically replaced by "element of a field F".

In 1-7, it has been supposed that "number" should mean "real number". This section forms a portion by itself; for the methods used there, it is essential that 0 cannot be represented as a sum of squares. This supposition is not satisfied in fields of characteristic p, and not even in every field of characteristic 0. The condition holds in the field of all the real numbers and in every subfield of it, but it is not satisfied in the field of all the complex numbers. The main-result of these considerations will be stated now as a theorem.

Theorem. Given any field F, then the investigations of 1-2 to 6 and 1-8 to 11 hold without any further alteration, if the notion of vectorspace is replaced by "vector-space V over F", n-vector by vector of V, and if the coefficients of the linear equations, the coordinates of the matrices and the terms of the determinants are supposed to be elements of F.

E.g. A vector α is considered to be *dependent* on the vectors $\beta_1, \ldots, \beta_m$ if $\alpha = b_1 \beta_1 + \ldots + b_m \beta_m$ holds, and the vectors $\beta_1, \ldots, \beta_m$ are independent if $c_1 \beta_1 + \ldots + c_m \beta_m = 0$ implies $c_1 = \ldots = c_m = 0$. The rank n of a vectors-space V is equal to the maximum number of independent vectors in V, and n is therefore independent of the choice of the basis of V.

2-63. *Finite extensions.* If a module R over a field F is itself a ring, then R is said to be a *ring over F*. In chapter VI, rings of matrices will be considered which are rings over the field of the coefficients of the matrices. A special case of great interest is when F is a subring of the ring R over F. In this case the unitelement of F is also the unitelement of R.

Let K be an arbitrary field, and let x be an indeterminate (the letter x not being used for denoting elements of K), the polynomials in x with coefficients of K form an integral domain K[x] which is a ring over K, and contains K as a subring. This ring is not a vectorspace, since the powers of x form an infinite set of independent elements; thus there exists no maximum number of independent elements in K [x] and therefore K [x] has no basis. The quotientfield of K [x] will be denoted by

$$\mathrm{K}\,(x). \tag{1}$$

This field is an extension of K, but it is not a vectorspace over K since it contains an infinite number of independent elements. Every extension of K which contains x, must contain every element of $K(x)$, and every ring over K which contains x must contain every element of $K[x]$. This notion can be generalised when x is an element which is not necessarily an indeterminate. Let Λ be an extension of K, and α be any element of Λ. If $f(x)$ runs over all the polynomials of $K[x]$, then the elements $f(\alpha)$ of Λ form a ring

$$K[\alpha], \tag{2}$$

and its quotientfield will be denoted by

$$K(\alpha). \tag{3}$$

Hence $K[\alpha]$ is the meet of all the rings containing K and α; similarly $K(\alpha)$ is the meet of all the extensions of K which contain α. The correspondence by which $f(x)$ is mapped on $f(\alpha)$, when $f(x)$ runs over $K[x]$, is a homomorphism ; thus $K[\alpha]$ is homomorphic to $K[x]$. If the field Λ is a vectorspace of rank, say n over K— i.e. if there esixts a maximum number n of independent elements in Λ —, then Λ is said to be *finite over* K. The rank n is denoted by

$$n = [\Lambda : K]. \tag{4}$$

In this case, there exists in Λ a *basis* $\alpha_1, \ldots, \alpha_n$ of Λ over K such that every element α of Λ can be represented in one and only one manner by $a_1 \alpha_1 + \ldots + a_n \alpha_n$ by the help of elements $a_1, \ldots, a_n$ of K. If an element α of Λ is a root of a polynomial of $K[x]$, then α is said to be *algebraic over* K, otherwise α is *transcendental over* K. If every element of Λ is algebraic over K, the extension Λ of K is said to be algebraic over K. The interconnection between these notions is shown in the following theorem.

Theorem. 1. If Λ is finite over K, it is algebraic over K. —
2. If α is algebraic over K, then $K(\alpha)$ is finite (and therefore algebraic) over K, and it is isomorphic to the field, formed by the classes of residues of the irreducible polynomial $f(x)$ of $K[x]$ of which α is a root ; furthermore $K(\alpha) = K[\alpha]$. The rank $[K(\alpha) : K] = n$ which is equal to the degree of $f(x)$, is said to be the *degree* of α over K ; $1, \alpha, \ldots, \alpha^{n-1}$ form a basis of Λ over K.—3. If α is transcendental over K, $K[\alpha]$ is isomorphic to $K[x]$, and therefore it is not a field.

Proof. (1) Let Λ be finite over K, say of rank n, and let β be any element of Λ. Then $1, \beta, \ldots, \beta^n$ cannot be independent ; hence a relation $c_0 + c_1 \beta + \ldots + c_n \beta^n = 0$ holds, where the coefficients $c_0, c_1, \ldots, c_n$ belong to K, and at least one of them is different from 0. Therefore $c_0 + c_1 x + \dots + c_n x^n = f(x)$ is not the polynomial 0 and $f(\beta) = 0$. Hence every element β of Λ is algebraic over K, and therefore Λ is algebraic over K.

(2) Let Λ be any extension of K, and α be an element of Λ which is algebraic over K. Then there exists a polynomial $\phi(x)$ in K $[x]$ such that $\phi(\alpha) = 0$. $\phi(x)$ is a product of irreducible factors $\phi(x) = f(x)\ f_1(x) \dots f_m(x)$. Therefore $f(\alpha)\ f_1(\alpha) \dots f_m(\alpha) = 0$, and as the factors on the left hand side are elements of the field Λ, one of the factors is zero, say $f(\alpha) = 0$, where $f(x)$ is irreducible and of degree, say n. The ring K $[\alpha]$ is homomorphic to K $[x]$. The subring R of K $[x]$ which is mapped on the zero-element of K $[\alpha]$ contains $f(x)$ and all the polynomials divisible by it, but no element of K besides 0. Since K $[x]$ is a Euclidean domain, R contains the *h. c. f.* of any two of its elements, and since R does not contain 1, it cannot contain any element which is relatively prime to $f(x)$; thus R contains those and only those elements of K $[x]$ which are divisible by $f(x)$. Hence two elements of K$[x]$ are mapped on the same element of K$[\alpha]$ if and only if their difference is divisible by $f(x)$. K $[\alpha]$ is therefore isomorphic to the ring of the classes of residues of $f(x)$ in K $[x]$. Since $f(x)$ is irreducible in K $[x]$, this ring is a field (see 2-47, th. 4). Hence K$[\alpha] \neq$ K (α) and [K(α) : K] $=$ n. In every class of residues there exists one and only one polynomial of degree $<$ n say $b_0 + b_1 x + \dots + b_{n-1}$ (see 2-47). The elements of K (α) can therefore be represented in one and only one manner by $b_0 + b_1 \alpha + \dots + b_{n-1} \alpha^{n-1}$. Hence $1, \alpha, \dots, \alpha^{n-1}$ is a basis of K (α) over K.

(3) Let α be transcendental over K. K$[\alpha]$ is homomorphic to K$[x]$. The ring R of the elements of K$[x]$ mapped on 0 does not contain any element of K other than 0. Let R contain a polynomial $f(x)$ of degree > 0, then $f(\alpha) = 0$, and this implies that α is algebraic over K. Since α is supposed to be transcendental, R contains the element 0 only, and therefore the homomorphism is an isomorphism. Hence the theorem.

2-64. *Rank of a field over a field.*

Theorem. Let Λ be a finite extension of K, and M be a finite extension of Λ, then M is a finite extension of K, and

$$[\mathrm{M} : \mathrm{K}] = [\mathrm{M} : \Lambda]\,[\Lambda : \mathrm{K}] \tag{1}$$

holds.

Proof. Let $\alpha_1, \dots, \alpha_n$ be a basis of Λ over K, and $\beta_1 \dots, \beta_m$ be a basis of M over Λ; then n $= [\Lambda : \mathrm{K}]$ and m $= [\mathrm{M} : \Lambda)$. Any element γ of M can be represented by $\gamma = \Sigma\lambda_i\, \beta_i$, where $\lambda_1, \dots, \lambda_m$ are elements of Λ and therefore $\lambda_i = \Sigma c^i_j \alpha_j$, where each c^i_j is an element of K. Hence $\gamma = \Sigma c^i_j \alpha_j \beta_i$. To prove that the n m elements of $\alpha_j \beta_i$ form a basis of M over K, one has therefore to prove only that they are independent. Suppose now $0 = \sum_{i,j} d^i_j \alpha_j \beta_i = \sum_i \beta_i \sum_j d^i_j \alpha_j$. Since in the last sum, the coefficients of β_i are elements of Λ, and $\beta_1, \ldots, \beta_m$ are independent, these coefficients are equal to zero. Similarly $\Sigma d^i_j \alpha_j = 0$ implies $d^i_j = 0$. Hence the n m elements are independent and form a basis of M over K. Hence the theorem.

Corollaries.

1. If Λ is a subfield of M and an extension of K, and M is finite over K, then M is finite over Λ, Λ is finite over K, and (1) holds.

Proof. As M is finite over K, say of rank q, and the elements of Λ belong to M, no set of more than q elements of Λ can be independent over K. Hence Λ is finite over K. Similarly every set of more than q elements of M is connected by a linear homogeneous equation, the coefficients being elements of K —and therefore elements of Λ— of which at least one is different from 0. Hence M is finite over Λ, and (1) follows from the above theorem.

2. If $[\Lambda : K] = q$, then the degree over K of any element α of Λ is a factor of q.

Proof. $[\Lambda : K(\alpha)]\ [K(\alpha) : K] = q$.

3. If $\phi(x)$ is a polynomial of $K[x]$, and $[K(\alpha) : K] = q$, then $[K(\phi(\alpha)) : K]$ is a factor of q.

4. If $[K(\alpha) : K] = p$ is a primenumber, and $0 <$ degree $\phi(x) < p$, then $K(\phi(\alpha)) = K(\alpha)$.

Proof. From the inequality it follows that $\phi(\alpha)$ is not an element of K. Hence $[K(\phi(\alpha)) : K] > 1$ and it is therefore equal to p. Hence $[K(\alpha) : K(\phi(\alpha))] = 1$. Hence the proposition.

2·65. *Highest common factor and extension of a field.* If F' is an extension of F, and $f_1(x)$ is a polynomial of $F[x]$, then it is also a polynomial of $F'[x]$. If a polynomial $f(x)$ of $F[x]$ is a factor of $f_1(x)$ in the ring $F[x]$, it is also a factor of $f_1(x)$ in $F'[x]$; if on the other hand $f(x)$ is a factor of $f_1(x)$ in $F'[x]$, one gets the quotient of the polynomials by the algorithmus of division; these coefficients therefore belong to F_1; hence $f_1(x)$ is divisible by $f(x)$ also in $F[x]$. However $f_1(x)$ may have factors which are polynomials in $F'[x]$ without belonging to $F[x]$. Let $f_1(x)$

and $f_2(x)$ be two polynomials of $F[x]$. The highest common factor $(f_1(x), f_2(x))$ can be calculated by the algorithmus of the *h. c. f.* its coefficients are obtained by rational operations and belong therefore to F; a common factor of those coefficients which is any element $\neq 0$ of F, remains arbitrary. If one considers $f_1(x)$ and $f_2(x)$ as elements of $F'[x]$, then the algorithmus furnishes the same polynomial $(f_1(x), f_2(x))$, but a common factor of the coefficients remains arbitrary which is an element $\neq 0$ of F'. Hence

Theorem. Let F' be an extension of F, and $f_1(x)$, $f_2(x)$ and $f(x)$ be elements of $F[x]$. A highest common factor of $f_1(x)$ and $f_2(x)$ in the ring of polynomials $F[x]$ is also a *h. c. f.* of those polynomials in $F'[x]$. If $f(x)$ is a factor of $f_1(x)$ in $F'[x]$, it is also a factor of $f_1(x)$ in $F[x]$ and conversely.

2·66. *Multiple roots.* Let α be a root of a ploynomial $f(x)$ of $K[x]$ and let $K(\alpha) = \Lambda$, then $f(x)$ can be represented in $\Lambda[x]$ by

$$f(x) = (x - \alpha) f_1(x).$$

Hence $f(x)$ is divisible by $(x-\alpha)^2$ if and only if $f_1(\alpha) = 0$. Denoting the derivatives in the usual manner:

$$f'(x) = f_1(x) + (x - \alpha) f'_1(x)$$

and therefore

$$f'(\alpha) = f_1(\alpha).$$

Thus $f'(\alpha) = 0$ is the necessary and sufficient condition for $f(x)$ to be divisible by $(x-\alpha)^2$. If

$$f(x) = \sum_0^n a_j \; x^j, \text{ then } f'(x) = \sum_1^n j \, a_j \; x^{j-1}.$$

Except for the case that $f(x)$ is 0, the degree of $f'(x)$ is less than the degree of $f(x)$. It may be remembered that the factor j means a sum of j terms, each being equal to the unitelement 1 of K (see 2·25, (3)); thus if the characteristic of K is zero, $j = 0$ implies j = 0, but if the characteristic is p, the element j is equal to zero if and only if j is divisible by p. Hence in the case of a characteristic $p \neq 0$ the degree of $f'(x)$ may differ by more than 1 from the degree of $f(x)$. Especially $f'(x) = 0$ if $j \, a_j = 0$, for $j = 0, 1, \ldots, n$. In the case when the characteristic is a primenumber p, this condition means that only the coefficients of terms x^{pq} can be different from zero. One can formulate this result in a manner which holds for both the cases:

Theorem 1. $f'(x) = 0$ if and only if

$$f(x) = \phi\,(x^{m}), \tag{1}$$

where m is the characteristic of K.

Indeed for $m = 0$, the condition means that $f(x)$ is of degree < 1, whereas for primenumber characteristic, the theorem has been proved just before.

Let $f(x)$ be irreducible and of degree > 0; consider the *h. c. f.* $(f(x), f'(x))$; then two cases have to be distinguished.

(1) $f'(x) \neq 0$, then $(f(x),\ f'(x)) = 1$.

(2) $f'(x) = 0$, then $(f(x),\ f'(x)) = f(x)$.

If again α is a root of $f(x)$, then $f'(\alpha) \neq 0$ in the first case and $f'(\alpha) = 0$ in the second case. Hence :

Theorem 2. Let $f(x)$ be an irreducible polynomial of $K[x]$, and let α be a root of it. Then $f(x)$ is divisible by $(x - \alpha)^2$ if and only if K has a primenumber characteristic p, and $f(x)$ is a polynomial in x^p over K.

If $f(x)$ is not divisible by a factor $(x - \alpha)^2$ in any extension of K, then it is said to be *separable*, otherwise non-separable. Irreducible polynomials over a field of characteristic 0 are therefore separable, whereas irreducible polynomials over a field K of characteristic p are non-separable if and only if they belong to $K[x^p]$.

2·67. *Non-Separable Polynomials.* Let K be a field of characteristic p, and $f(x)$ be an irreducible polynomial over K, and of degree n. Then there exists a uniquely determined integral number $e \geqq 0$, such that $f(x)$ belongs to $K[x^{p^e}]$, but not to $K[x^{p^{e+1}}]$. Thus $f(x)$ is separable if and only if $e = 0$. At any rate

$$f(x) = \psi\,(x^{p^e}). \tag{1}$$

The polynomial $\psi(y)$ of $K[y]$ is irreducible as $\psi(y) = \psi_1(y)\ \psi_2(y)$ implies $f(x) = \psi_1(x^{p^e})\ \psi_2(x^{p^e})$. Moreover $\psi(y)$ cannot belong to $K[y^p]$, otherwise $f(x)$ must belong to $K[x^{p^{e+1}}]$. Hence $\psi(y)$ is irreducible and separable. Let q be the degree of $\psi(y)$, then

$$n = q\ p^e.$$

In a suitable extension Λ of K, the polynomial $\psi(y)$ can be represented by

$$\psi(y) = a(y-\beta_1)\ \ldots\ (y-\beta_q), \tag{2}$$

where $\beta_1, \dots, \beta_q$ belong to Λ, and a belongs to K. Hence

$$f(x) = a\,(x^{p^e} - \beta_1) \dots (x^{p^e} - \beta_q). \tag{3}$$

Since $\psi(y)$ is separable, $\beta_1, \dots, \beta_q$ are q different elements.

In a suitable extension M of Λ, there exist elements γ_j such that

$$\gamma_j^{p^e} = \beta_j, \text{ for } j = 1, \dots, q. \tag{4}$$

Since the characteristic of M is p (see 2·26, (2)),

$$(x - \gamma_j)^{p^e} = x^{p^e} - \gamma_j^{p^e} = x^{p^e} - \beta_j.$$

Hence

$$f(x) = a[(x - \gamma_1) \dots (x - \gamma_q)]^{p^e}. \tag{5}$$

Since the q elements β_j are different, it follows from (4) that $\gamma_1, \dots, \gamma_q$ are different. Hence:

Theorem. An irreducible polynomial $f(x)$ over a field K of characteristic p which is of degree n, has exactly $q = n : p^e$ different roots in a suitable extension of K and it can be represented by (5). The integral number $e \geqq 0$ is uniquely determined by the condition that $f(x)$ belongs to $K[x^{p^e}]$, but not to $K[x^{p^{e+1}}]$.

2·7. *Repeated extension of a field.*

2·71. *Extension of a field to a ring and to a field by a finite number of steps.* Let K be a subfield of Λ, and let

$$\alpha_1, \alpha_2, \dots, \alpha_m \tag{1}$$

be elements of Λ. Denote

$$K(\alpha_1) = K_1,\ K_1(\alpha_2) = K_2, \dots, K_{m-1}(\alpha_m) = K_m. \tag{2}$$

Thus K_1 is the meet of all extensions of K which contain α_1 (see 2·63), and K_2 is the meet of all the extensions of K_1 which contain α_2. Hence K_2 is an extension of K containing α_1 and α_2. On the other hand every extension K' of K which contains α_1 and α_2 is an extension of K_1, therefore K_2 is a subfield of K'; hence K_2 is the meet of all the extensions of K which contain α_1 and α_2. Similarly K_m is the meet of all those extensions of K which contain all the elements (1). One therefore denotes

$$K_m = K(\alpha_1, \dots, \alpha_m), \tag{3}$$

where the elements in the bracket can be interchanged among themselves arbitrarily.

Let $f(x_1, \dots, x_m)$ run over all the polynomials of $K[x_1, \dots, x_m]$ (see 2·36), then the elements $f(\alpha_1, \dots, \alpha_m)$ form a ring

$$K[\alpha_1, \dots, \alpha_m] \tag{4}$$

which is homomorphic to $K[x_1, \dots, x_m]$ and which is contained in K_m. The quotientfield of (4) is also contained in K_m. Since on the other hand the quotientfield is an extension of K containing the m elements (1), it must be identical with K_m. Hence every element of K_m can be represented in the form

$$f(\alpha_1, \dots, \alpha_m) : \phi(\alpha_1, \dots, \alpha_m), \tag{5}$$

where the numerator runs over all the elements of (4), and the denominator over those elements of (4) which are different from zero. Though $K[\alpha_1, \dots, \alpha_m]$ is homomorphic to $K[x_1, \dots, x_m]$, the quotientfield $K(\alpha_1, \dots, \alpha_m)$ is in general not homomorphic to $K(x_1, \dots, x_m)$ as a field cannot be homomorphic to a field unless they are isomorphic. Of course, the correspondence

$$f(x_1, \dots, x_m) \rightarrow f(\alpha_1, \dots, \alpha_m)$$

cannot be extended to the correspondence

$$f(x_1, \dots, x_m) : \phi(x_1, \dots, x_m) \rightarrow f(\alpha_1, \dots, \alpha_m) : \phi(\alpha_1, \dots, \alpha_m)$$

if there are polynomials ϕ which are different from the null-polynomial and for which nevertheless $\phi(\alpha_1, \dots, \alpha_m) = 0$ holds. If there is no such polynomial, then $K(x_1, \dots, x_m)$ and $K(\alpha_1, \dots, \alpha_m)$ are isomorphic.

Theorem. If $\alpha_1, \dots, \alpha_m$ are algebraic over K, then

$$K(\alpha_1, \dots \alpha_m) = K[\alpha_1, \dots, \alpha_m].$$

Proof. (by mathematical induction). For $m=1$, the theorem has been proved in 2·63. Suppose $K[\alpha_1, \dots, \alpha_{m-1}] = K(\alpha_1, \dots, \alpha_{m-1}) = \Lambda$. Then α_m is algebraic over Λ, and $K[\alpha_1, \dots, \alpha_m] = \Lambda[\alpha_m] = \Lambda(\alpha_m) = K(\alpha_1, \dots, \alpha_m)$ holds.

Exercises. Let R be the field of the rational numbers.

(1). Consider $\Lambda = R(\sqrt{2}, \sqrt{3})$. Construct a basis of Λ and show that $\Lambda = R(\sqrt{2} + \sqrt{3})$.

(2) Investigate $R(\sqrt{2}, \sqrt[3]{2})$.

2·72. *Primitive element of an extension.* If

$$\Lambda = K(\alpha), \ [\Lambda : K] > 1,$$

then α is said to be a *primitive element of the extension* Λ *of* K. The examples given in the exercises just above show that even an extension generated by more than one step may have a primitive element. As a matter of fact, a finite extension of a field of characteristic 0 can always be performed by the help of a primitive element. The corresponding statement holds for a large class of fields of characteristic p; that this class includes all the finite fields, will be shown later in 3·21 by a different method. To investigate the case where K has an infinite number of elements, the following lemma is used.

Lemma. Let $f(x)$ and $g(x)$ be polynomials of $K[x]$ and let in a suitable extension of K,

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n), \; g(x) = (x - \beta_1) \dots (x - \beta_m); \qquad (1)$$

if c is such an element of K that for $i = 1, \dots, n$ and $k = 2, \dots, m$ the $n(m - 1)$ inequalities

$$\gamma = \alpha_1 + c\,\beta_1 \neq \alpha_i + c\,\beta_k \qquad (2)$$

hold, then

$$K(\gamma) = K(\alpha_1, \beta_1). \qquad (3)$$

Proof. Put $K(\gamma) = K'$; then $\phi(x) = f(\gamma - c\,x)$ is a polynomial of $K'[x]$ which has a root β_1 in common with $g(x)$. If β_k were a common root of $\phi(x)$ and $g(x)$, then $\gamma - c\,\beta_k = \alpha_i$, contrary to (2). Hence the h. c. f. $(\phi(x), g(x)) = x - \beta_1$, and therefore β_1 is an element of K′. Furthermore $\alpha_1 = \gamma - c\,\beta_1$ belongs to K′, thus every element of $K(\alpha_1, \beta_1)$ does. Since on the other hand γ belongs to $K(\alpha_1, \beta_1)$, the lemma follows.

Theorem. Let K be a field containing an infinite number of elements; let α be algebraic over K, and $\beta, \dots, \kappa$ be roots of separable polynomials of $K[x]$, then there exists a primitive element λ for the extension $K(\alpha, \beta, \dots, \kappa)$ of K.

Proof. At first will be proved that $K(\alpha, \beta) = K(\alpha')$. Put $\alpha = \alpha_1$, $\beta = \beta_1$, and let $f(x)$ and $g(x)$, as represented by (1), be the irreducible polynomials in $K[x]$ with the roots α and β respectively. Since $g(x)$ is supposed to be separable, the roots $\beta_1, \beta_2, \dots, \beta_m$ are all different. To determine α', one has to find out an element b of K such that

$$\alpha' = \alpha_1 + b\,\beta_1 \neq \alpha_i + b\,\beta_k \text{ for } i = 1, \dots, n, \; k = 2, \dots, m.$$

These conditions are satisfied, if b is not a root of anyone of the linear equations

$$(\alpha_1 - \alpha_i) + x(\beta_1 - \beta_k) = 0. \qquad (4)$$

Since $\beta_1 - \beta_k \neq 0$, each of these equations has exactly one solution in a suitable extension of K, and therefore at most one solution in K. Now K contains an infinity of elements, hence there exists an element b in K which does not satisfy anyone of the n(m − 1) equations (4). Hence α' is a primitive element of the extension $K(\alpha, \beta)$ of K. Since α and β are algebraic over K, the extension $K(\alpha)$ is finite over K, and $K(\alpha') = K(\alpha, \beta)$ is finite over $K(\alpha)$ and therefore finite over K. Hence α' is algebraic over K. Thus $\Lambda = K(\alpha', \ldots, \kappa)$, where α' is algebraic over K, and the other elements in the bracket are roots of separable polynomials. The procedure can therefore be repeated, till the number of the elements in the bracket is reduced to one element

$$\lambda = \alpha + b\ \beta \ldots + k\ \kappa$$

$$K(\alpha, \beta, \ldots, \kappa) = K(\lambda).$$

If in particular, the characteristic of K is 0, then K has an infinite number of elements, and every irreducible polynomial is separable. Thus one gets immediately the following corollary.

Corollary. If K is a field of characteristic 0, and $\alpha, \beta, \ldots, \kappa$ are algebraic over K, then there exists a (primitive) element λ, such that $K(\alpha, \beta, \ldots, \kappa) = K(\lambda)$ holds.

2-73. *Extension by roots of two different irreducible polynomials.* In 2-71 and 2-72, such extensions of a field K have been considered which are generated by elements $\alpha, \beta, \ldots$ of any field of which K is a subfield. In an earlier section extensions of a different kind have been used already. One can extend a field K to a field $K(\alpha)$ where α is not given, but has to be created in such a way that it is a root of a polynomial $f(x)$ of $K[x]$. It has been proved in 2-51 that this extension is always possible and in 2-52 it was shown that if $f(x)$ is irreducible, the extension is determined uniquely in the sense of isomorphism.

The first statement can be generalised without difficulty to the case of more than one polynomial. Given polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ in $K[x]$, then one can construct by repeated extension a field $K(\alpha, \beta, \ldots, \kappa)$ such that $0 = f_1(\alpha) = f_2(\beta) = \ldots = f_k(\kappa)$. Let now the k polynomials be irreducible in K, then $K(\alpha)$ is determined uniquely in the sense of isomorphism but $f_2(x)$ — though irreducible in K—may be reducible in $K(\alpha)$. Let $f_2(x) = \phi_1(x)\,\phi_2(x)$, furthermore let β be a root of $\phi_1(x)$, and β' a root of $\phi_2(x)$, then it is not certain whether $K(\alpha, \beta)$ and $K(\alpha, \beta')$ are isomorphic or not. That both the cases occur is shown by the following examples on extensions of the field R of the rational numbers.

1. $f_1(x) = x^2 - 2,\ f_2(x) = x^4 - 2.$

$$\alpha^2 = 2, \qquad f_2(x) = (x^2 - \alpha)(x^2 + \alpha);\ R(\alpha) = \mathrm{K}_1$$

$$\beta^2 = \alpha,\ \beta'^2 = -\alpha;\ \mathrm{K}_1(\beta) = R(\beta),\ \mathrm{K}_1(\beta') = R(\beta').$$

Hence $R(\alpha, \beta)$ and $R(\alpha, \beta')$ are isomorphic. It may be mentioned that these two isomorphic fields of numbers are different fields; the first is a field of real numbers only, whereas the second contains complex numbers.

2. $f_1(x) = x^3 - 2,\ f_2(x) = x^6 - 2;$

$$\alpha^3 = 2, \qquad f_2(x) = (x^2 - \alpha)(x^4 + \alpha x^2 + \alpha^2);\ R(\alpha) = \mathrm{K}_1$$

$$\beta^2 = \alpha,\ \beta'^4 + \alpha\beta'^2 + \alpha^2 = 0;\ \mathrm{K}_1(\beta) = \mathrm{K}_2,\ \mathrm{K}_1(\beta') = \mathrm{K}'_2.$$

K_2 is composed of real numbers; hence 0 cannot be represented as a sum of squares of elements of K_2 which are different from 0, nor can 0 be represented in that manner in any field which is isomorphic to K_2. In K'_2 however

$$(2\beta'^2 + \alpha)^2 + \alpha^2 + \alpha^2 + \alpha^2 = 4(\beta'^4 + \alpha\beta'^2 + \alpha^2) = 0$$

holds. Hence K'_2 is non-isomorphic to K_2. Thus it is possible that a field K can be extended to two non-isomorphic fields by roots of the same two polynomials both irreducible in K.

2·74. *Normal extension of a field.* A case of special interest is when a field K is to be extended by n different roots of *one* polynomial of degree n. In this case, a theorem of uniqueness (in the sense of isomorphism) holds, and one is led to the *normal extensions* of a field which play a very important role in algebra. For these investigations the following three definitions will be needed:

Definition 1. Let I' be an isomorphism mapping a field K on a field Λ; then a subring R of K is mapped on a subring L of Λ. This mapping of R on L is an isomorphism of R to L, say the isomorphism I. Then the isomorphism I' is called an *extension* of the isomorphism I.

Often the problem occurs of finding an extension I' to a given isomorphism I.

Definition 2. Let $f(x)$ be a polynomial of $\mathrm{K}[x]$, then there exists an extension M of K, in which $f(x)$ is a product of linear factors. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in M, then $f(x)$ can be represented as a product of linear factors only in those subfields of M, which contain $K(\alpha_1, \ldots, \alpha_n)$. This field is therefore said to be a *smallest extension of* K *admitting the complete reduction of* $f(x)$.

Theorem 1. Let K and Λ be isomorphic, $f(x)$ and $\phi(x)$ be corresponding polynomials of $K[x]$ and $\Lambda[x]$. Let K' be a smallest extension of K admitting the complete reduction of $f(x)$, and let Λ' be a smallest extension of Λ admitting the complete reduction of $\phi(x)$; then every isomorphism I of K and Λ can be extended to an isomorphism I' of K' and Λ'.

Proof. The theorem holds obviously if $[K' : K] = 1$ since in this case $K = K'$, and $\Lambda = \Lambda'$. To prove the theorem by mathematical induction, it will be supposed to hold for $[K' : K] < m$. Let $[K' : K] = m$, and $f_1(x)$ be an irreducible factor of $f(x)$ of degree > 1. Let $\phi_1(x)$ be the polynomial of $\Lambda[x]$ isomorphic to $f_1(x)$, let α be a root of $f_1(x)$ in K', and let β be a root of $\phi_1(x)$ in Λ'. We can extend the isomorphism I to an isomorphism of the classes of residues of $f_1(x)$ in $K[x]$ and of $\phi_1(x)$ in $\Lambda[x]$, and therefore to an isomorphism I_1 of $K(\alpha)$ and $\Lambda(\beta)$. Every extension of $K(\alpha)$ admitting the complete reduction of $f_1(x)$ is an extension of K admitting the complete reduction of $f(x)$; hence K' is a smallest extension of $K(\alpha)$ admitting this reduction. For the same reason Λ' is a smallest extension of $\Lambda(\beta)$ admitting the complete reduction of $\phi(x)$. As $[K' : K(\alpha)] < m$, the isomorphism I_1 can be extended to an isomorphism I' of K and Λ', and since I' is an extension of I, the theorem holds.

This theorem can be applied also to the cases when K and Λ are identical, and I maps every element of K on itself. So one gets the following important corollary.

Corollary. Any two smallest extensions of K admitting the complete reduction of a polynomial $f(x)$ of $K[x]$ are isomorphic. The isomorphism can be chosen in such a way that every element of K is represented by itself.

Definition 3. Let N be an extension of K with the property that every irreducible polynomial of $K[x]$ which has a root in N can be represented in $N[x]$ as a product of polynomials of degree 1, then N is called a *normal extension* of K.

Theorem 2. If K' is a smallest extension of K admitting the complete reduction of an arbitrary polynomial $f(x)$ of $K[x]$, then K' is a normal extension of K.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in K′, let $g(x)$ be irreducible in K, let β and β' be roots of $g(x)$, and let β belong to K′. It will be shown that β' also belongs to K′. If not so, then β' belongs to a suitable extension of K′. Therefore $K_1 = K(\beta)$ and $K_2 = K(\beta')$ are isomorphic, and there exists an isomorphism I of these fields by which every element of K corresponds to itself, and β corresponds to β'. From theorem 1 it follows, that one can extend I to an isomorphism I' of $K_2(\alpha_1, \ldots, \alpha_n)$ and $K_1(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n) = K'$. By I' every root of a polynomial with coefficients from K will be represented by a root of the same polynomial; hence the elements α_i will only be interchanged. Put $\beta = F(\alpha_1, \ldots, \alpha_n)$, where the coefficients of F are elements of K. Hence $\beta' = F(\alpha_{k_1}, \ldots, \alpha_{k_n})$, and therefore β' belongs to K′. Since β' is supposed to be an arbitrary root of $g(x)$, the theorem holds.

*2·741. *Generalisations of the theorem on normal extensions*. Consider now two different generalisations of this theorem.

Theorem 1. Let $f_1(x), f_2(x), \ldots$ be a sequence of polynomials of $K[x]$, finite or infinite in number; the smallest extension of K admitting the complete reduction of all these polynomials is a normal extension of K.

Proof. Let $F_m(x) = f_1(x)\, f_2(x) \ldots f_m(x)$, and let K_m be the normal extension obtained by extending K with the roots of $F_m(x)$, $m = 1, 2, \ldots$. Now K_1 is a subfield of K_2, again K_2 a subfield of K_3, and so on; the smallest extension of K admitting the complete reduction of all the $f_m(x)$ is the join of the fields K_m, *i.e.* the set of all those elements which belong to any field K_m, for $m = 1, 2, \ldots$ This set is a field K^*. If therefore a polynomial $g(x)$ has a root in K^*, this root is an element of a suitable K_m, and since K_m is a normal extension of K, the polynomial $g(x)$ is a product of linear polynomials in K_m and in every extension of K_m, in particular in K^*. Hence the theorem holds.

The second generalisation concerns the factorisation of $g(x)$ in a field N, which is normal and algebraic over K when $g(x)$ is irreducible in $K[x]$. Let $\psi_1(x), \ldots, \psi_m(x)$ be irreducible factors of $g(x)$ in N, let β_1 be a root of $\psi_1(x)$ and β_2 a root of $\psi_2(x)$ in a suitable extension of N. The coefficients of $\psi_1(x)$ are roots of polynomials $f_1(x), \ldots, f_t(x)$, irreducible in K. As N is normal over K, the roots of every $f_i(x)$ belong all to N. Let $\alpha_1, \ldots, \alpha_n$ be these roots; then $K \subseteq K(\alpha_1, \ldots, \alpha_n) = \Lambda \subseteq N$. Λ is a finite extension of K and normal over K; the factorisation of $g(x)$ in Λ is the same as in N.

---

* May be omitted at the first reading.

As β_1 and β_2 are roots of $g(x)$, irreducible in K, the fields $K(\beta_1)$ and $K(\beta_2)$ are isomorphic, and there is an isomorphism by which β_1 is represented by β_2, and the elements of K do not change. Hence no $f_i(x)$ is changed by it. We can extend this isomorphism to an isomorphism of $K(\beta_1, \alpha_1, \ldots, \alpha_n) = \Lambda(\beta_1)$ and $K(\beta_2, \alpha_1, \ldots, \alpha_n) = \Lambda(\beta_2)$. By this isomorphism, every $f_i(x)$ remains invariant ; its roots are therefore interchanged only; hence an element of Λ is represented by an element of Λ. The polynomial $\psi_1(x)$ which is irreducible in Λ and which is a factor of the polynomial $g(x)$, irreducible in K, must therefore be represented by a factor of $g(x)$ which is irreducible in Λ. Since the root β_1 of $\psi_1(x)$ is represented by the root β_2 of $\psi_2(x)$, the image of $\psi_1(x)$ is $\psi_2(x)$, and as these two polynomials are arbitrary irreducible factors of $g(x)$, the following theorem holds :

Theorem 2. If $g(x)$ is irreducible in K, and N is normal and algebraic over K, every irreducible factor of $g(x)$ in N can be transformed into every other by a suitable automorphism of a certain field over K; hence these factors are all of the same degree.

If one of the irreducible factors is of degree 1, the others are also linear ; so 2·74, theorem 2 is a special case of this theorem.

2·742. *Automorphisms of a normal extension.* Let $N = K(\alpha_1)$ be a normal extension of K, and $[N : K] = n$. Then $1, \alpha_1, \ldots, \alpha_1^{n-1}$ form a basis of N over K, and therefore α_1 is the root of a polynomial of degree n which is irreducible in $K[x]$,

$$f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n.$$

As N is a normal extension of K, and it contains a root of $f(x)$, this polynomial is factorised in $N[x]$ by

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

Since $K(\alpha_j)$ is isomorphic to $K(\alpha_1)$, so $[K(\alpha_j) : K] = n$; furthermore α_j and therefore every element of $K(\alpha_j)$ are contained in $K(\alpha_1)$, hence $[K(\alpha_1) : K(\alpha_j)] = 1$. Therefore

$$N = K(\alpha_1) = \ldots = K(\alpha_n)$$

holds. There exists an isomorphism mapping $K(\alpha_1)$ on $K(\alpha_j)$ by which the elements of K remain unaltered. This isomorphism is an automorphism of N. On the other hand, if there is an automorphism of N for which the elements of K remain fixed, $f(x)$ is transformed into itself and therefore every root of $f(x)$ is mapped on a root of $f(x)$. The roots of $f(x)$ are therefore undergoing a permutation by the automorphism, and the automorphism is uniquely determined by the condition that α_1 is to be mapped on α_j since this condition implies that the basis $I, \alpha_1, \ldots, \alpha_1^{n-1}$ is mapped on the basis $I, \alpha_j, \ldots, \alpha_j^{n-1}$. Hence there exist exactly n automorphisms of N for which the elements of K remain invariant. For $n > 2$, not every permutation of the roots of $f(x)$ corresponds to one of these automorphisms. There exists one and only one automorphism of N for which the elements of K remain invariant and a particular root of $f(x)$, say α_1, is transformed into any particular root, say α_j. For $n = 1$ this automorphism is the identity. If in particular K is of characteristic 0, and M is a finite and normal extension of K, then there exists a primitive element α[see 2-72] such that $M = K(\alpha)$ and the above statements on automorphism hold.

Moreover, let K be an arbitrary field, $[\Lambda : K] = 2$, and β_1 be an element of Λ which does not belong to K. Then $\Lambda = K(\beta_1)$ [see 2-64, corollary 4]. β_1 is a root of a polynomial of degree 2, say $f(x)$, which is irreducible in K, but reducible in Λ

$$f(x) = (x - \beta_1)\,(x - \beta_2).$$

Hence β_2 belongs to Λ. An extension of rank 2 is therefore always a normal extension. Besides the identity, there exists one automorphism A of Λ for which K remains invariant. A interchanges β_1 and β_2, and since I, β_1 is a basis of Λ over K, one can express A by

$$\alpha = a + b\,\beta_1 \longleftrightarrow a + b\,\beta_2 = \bar{\alpha},$$

where a and b run over K. The elements α and $\bar{\alpha}$ are said to be *conjugate*. Conjugacy is a symmetric relation, because every element is the conjugate of its conjugate. The elements of K are the only ones which are self-conjugate. The remaining elements of Λ consist of pairs of conjugate elements.

CHAPTER III

GENERAL ALGEBRA, SPECIFIED THEORY

3-1. *Cyclotomic polynomials.*

The following equation plays an important role in algebra

$$x^n - 1 = 0. \tag{1}$$

As 1 may be the unitelement of any field K, the polynomial on the left hand side of (1) can be considered as belonging to any ring of polynomials $K[x]$. To investigate (1), the nature of the field K has therefore to be taken into account. If K is the field of the complex numbers, then the solutions of (1) are

$$e^{2k\pi i : n} = \cos 2\pi \frac{k}{n} + i \sin 2\pi \frac{k}{n}, \tag{2}$$

$$\text{for } k = 1, \ldots, n.$$

By representing these points in the complex plane in the usual manner, one gets n points which subdivide the unitcircle into n equal arcs. The problem of partitioning a circle into congruent arcs, leads therefore to the equation (1). Here, the equation will be considered from a purely algebraic point of view.

3-11. *Reduction of the problem to the case when* n *is not divisible by the characteristic.* For $f(x) = x^n - 1$, $f'(x) = n\, x^{n-1}$. The highest common factor is therefore found to be

$$\begin{aligned} (\, f(x), f'(x)\,) &= f(x) \text{ if } n \text{ is divisible by the characteristic of K} \\ &= 1 \text{ if } n \text{ is not divisible by the characteristic of K.} \end{aligned} \tag{1}$$

In the 2^{nd} case, $f(x)$ has n different roots.

Suppose at first that n is divisible by the characteristic of K : this is possible only if the characteristic is a primenumber, say p.

Put

$$n = p^e\, m, \text{ where } e > 0,\ (p, m) = 1 \tag{2}$$

and

$$g(x) = x^m - 1. \tag{3}$$

Since $(g(x), g'(x)) = 1$, the polynomial $g(x)$ is separable (see 2·6) and it has therefore m different roots in a suitable extension of K. As furthermore the characteristic of K is equal to p,

$$(g(x))^{p^e} = x^{mp^e} - 1 = f(x).$$

Hence $f(x)$ has the same roots as $g(x)$ has ; each of these roots occurs once as a root of $g(x)$, and p^e times as a root of $f(x)$. Thus the problem has been reduced to the case where n is not divisible by the characteristic of K.

3·12. *Primitive roots.* Suppose now that n is not divisible by the characteristic of K; this supposition holds *e. g.* when the characteristic is 0. In any field admitting the complete reduction of $f(x)$, this polynomial has therefore n different roots. The same holds for $x^h - 1 = 0$, where h is an arbitrary factor of n.

Let α and β be roots of $f(x)$, thus $\alpha^n = 1 = \beta^n$; hence $(\alpha\beta)^n = 1$, $(\alpha : \beta)^n = 1$. The roots of $f(x)$ therefore form a multiplicative abelian group Γ. Let r be the smallest positive integer for which $\alpha^r = 1$ holds, then r is said to be the *order* of α in Γ. As $\alpha^{sr+tn} = 1$ for every pair of integers s and t, $\alpha^m = 1$, where $m = (r, n)$. Hence $m \geqq r$, and therefore r is a factor of n. On the other hand, if r is a factor of n, then the roots of $x^r - 1$ are at the same time roots of $x^n - 1$. The elements of Γ of order n are called *primitive roots* of $f(x)$; the number of these primitive roots will be denoted by $\varphi(n)$.

To prove that for every n, primitive roots exist, one has to show that $\varphi(n) > 0$. In the following, the value of $\varphi(n)$ will be calculated ; it will be shown to be equal to a well known function of the elementary theory of numbers and to take positive values only.

Let α be a root of order h, and $0 < t$. Put $\beta = \alpha^t$, $(t, h) = r = at + bh$, and $h : r = s$, $t : r = u$, then $\beta^s = \alpha^{urs} = 1$ on the other hand, let $0 < s' < s$;

then
$$\beta^{s'a} = \alpha^{ts'a} = \alpha^{rs'} \neq 1,$$

since $0 < r s' < h$; hence $\beta^{s'} \neq 1$, and s is the order of α^t. Thus those and only those elements α^t are of order h, for which $(t, h) = 1$. Now α is a primitive root of $x^h - 1$. Hence if there exists a primitive root, the number of all the primitive roots is equal to the number of the natural numbers which are smaller than the exponent and relatively prime to it. Let Λ be an extension of K admitting the complete reduction of $f(x) = x^n - 1$, and let α be a root of order h, β be a root of order k and $(h, k) = 1$. Consider the h k products

$$\alpha^r \beta^s, \text{ for } r = 0, \ldots, h-1, \ s = 0, \ldots, k-1. \tag{1}$$

Now $\alpha^r \beta^s = \alpha^{r'} \beta^{s'}$ implies $\alpha^{r-r'} = \beta^{s'-s}$. The left hand side has an order which is a factor of h, whereas the order of the element on the right is a factor of k ; since (h, k) = 1, the order of both the sides must be 1: the two sides are therefore equal to 1. Hence $r - r' = s' - s = 0$. Thus the h k elements (1) are all different, they form therefore a full system of roots of the polynomial $x^{hk} - 1$. Now it will be proved that $\alpha\,\beta$ is of order $h\,k$.

Let $(\alpha\beta)^u = \alpha^r \beta^s$, where $r \equiv u$ (mod. h) and $s \equiv u$ (mod. k) and r, s satisfy the same conditions as in (1). As the elements $\alpha^r \beta^s$ are all different, $(\alpha\,\beta)^u = 1$ implies $r = s = 0$; therefore u must be divisible by h and k, therefore by h k. Hence the order of the root $\alpha\,\beta$ is equal to h k ; the same holds for the elements

$$\alpha^r \beta^s, \text{ for which } (r, h) = 1, \ (s, j) = 1 \tag{2}$$

as in this case α^r is of order h, and β^s of order k. If however $(r, h) = v > 1$, then $(\alpha^r \beta^s)^{hk:v} = 1$ and $\alpha^r \beta^s$ is of a smaller order than h k ; similarly if s is not relatively prime to k. Hence the elements (2) are the only ones of order h k, and therefore the only primitive roots of $x^{hk} - 1$. Hence

$$\phi(h\,k) = \phi(h)\,\phi(k), \quad \text{for } (h, k) = 1. \tag{3}$$

This formula can immediately be generalised to a product of any number of factors, where the arguments are relatively prime.

Especially

$$\phi(q_1^{k_1} q_2^{k_2} \ldots q_m^{k_m}) = \phi(q_1^{k_1})\,\phi(q_2^{k_2}) \ldots \phi(q_m^{k_m}), \tag{4}$$

where $q_1, q_2, \ldots, q_k$ are all different primenumbers.

To determine $\phi(q^k)$, where q is a primenumber, consider a root α of $x^{q^k} - 1$ which is non-primitive. Then $\alpha^{q^{k-1}} - 1 = 0$. There are q^{k-1} elements of Λ satisfying this condition. The number of the primitive roots is therefore $q^k - q^{k-1}$. Hence

$$\phi(q^k) = q^k\left(1 - \frac{1}{q}\right). \tag{5}$$

From (4) and (5) follows

$$\phi(n) = n \prod \left(1 - \frac{1}{q_k}\right) > 0, \tag{6}$$

where $q_1, \ldots, q_m$ are different prime-factors of n. The essence of these considerations is given by the following theorem :

Theorem. If $x^n - 1$ is a polynomial of K[x], and the characteristic of K is not a factor of n, then this polynomial has n different roots. There are $\phi(n)$ primitive roots of $x^n - 1$; $\phi(n)$ is equal to the number of the positive integers $< n$ which are relatively prime to n and is given by (6). Each root of $x^n - 1$ is a power of every arbitrary primitive root of that polynomial.

3·13. *Cyclotomic polynomials of order* n. Let $r_1, r_2, \ldots, r_m$ be the divisors of n which are different from n and $(x^n - 1) : (x^{r_i} - 1) = \psi_i(x)$, then the *h. c. f.* of all the polynomials $\psi_i(x)$ is a polynomial whose roots are just the primitive roots of $x^n - 1$. This polynomial is called a *cyclotomic polynomial of order* n ; its degree is $\phi(n)$.

To calculate a cyclotomic polynomial, it is not always necessary to compute all the polynomials $\psi_i(x)$.

Example n = 12.

The non-primitive roots of $(x^{12} - 1)$ are either roots of $(x^6 - 1)$, or of $(x^4 - 1)$, the common factor of both polynomials being $(x^2 - 1)$. Hence the cyclotomic polynomial of order 12 is $((x^{12} - 1) : (x^6 - 1)) : ((x^4 - 1) : (x^2 - 1)) = (x^6 + 1) : (x^2 + 1) = x^4 - x^2 + 1$.

Theorem. If α is a root of $x^n - 1$, K(α) is a normal extension of K.

Proof. Even if n is divisible by the characteristic of K, (see 3·11), α is a root of a polynomial $x^m - 1$, where m is not divisible by the characteristic. The order of the root α is a factor, say h of m (possibly h = m) ; thus α is a primitive root of $x^h - 1$. The roots of this polynomial are powers of α and therefore contained in K(α). This field is therefore a smallest extension of K admitting the complete reduction of $x^h - 1$. Hence the theorem follows from 2·74, theorem 2.

The factorisation of the cyclotomic polynomials, especially its irreducibility in a primefield of characteristic 0 will be considered in 3·433.

3·2. *Galoisfields.*

3·21. *Fundamental properties.* A field Γ which contains only a finite number of elements is called a *Galoisfield*. As the primefield of Γ is finite, the characteristic of Γ must be a primenumber, say p. The primefields GF_p of characteristic p themselves are instances of Galoisfields. Γ must be finite over its primefield GF_p, otherwise it would contain an infinite number of elements. Hence Γ is algebraic over GF_p(see 2·63), and there exists a finite basis of say n elements

$$\alpha_1, \ldots, \alpha_n \qquad (1)$$

of Γ, so that every element of Γ can be represented in one and only one manner by

$$\beta = b_1 \alpha_1 + \ldots + b_n \alpha_n, \tag{2}$$

where $b_1, \ldots, b_n$ are elements of GF_p. Hence Γ has exactly p^n different elements, where p is the characteristic of Γ and $n = [\Gamma : GF_p]$. The elements $\neq 0$ of Γ form a multiplicative abelian group A with $p^n - 1$ elements. Let β be an element of A; then $\beta, \beta^2, \ldots$ cannot be all different. From $\beta^a = \beta^b$ it follows $\beta^{a-b} = 1$. Hence each element of A is a root of a cyclotomic equation. Let r be the order of β, hence $\beta, \beta^2, \ldots, \beta^r$ are all different. Let two elements γ and δ be considered as equivalent elements if $\delta\gamma^{-1} = \beta^i$, then this equivalence defines a partition of A in classes (see 2-13). Each class contains r different elements. Let s be the number of the classes, then $rs = p^n - 1$ holds. Hence the order of every element of A is a factor of $p^n - 1$, and therefore every element of A is a root of $x^{p^n-1} - 1$. As the polynomial cannot have more than $p^n - 1$ roots in Γ, every root is an element of A. So the elements of Γ are identical with the roots of $x^{p^n} - x$, and

$$x^{p^n} - x = \prod_{i=1}^{p^n} (x - \beta_i), \tag{3}$$

where β_i are elements of Γ.

Let α be a primitive root of $x^{p^n-1} - 1$, then

$$\Gamma = GF_p(\alpha) \tag{4}$$

is a normal field over GF_p, because it is the smallest extension admitting the complete reduction of $x^{p^n-1} - 1$. From 2-52 it follows, that all Galoisfields with p^n elements are isomorphic. For this reason, (4) will also be denoted by

$$GF_{p^n}. \tag{4'}$$

To prove that to every p^n there exists a Galoisfield GF_{p^n}, it suffices to show that in every field of characteristic p which admits the complete reduction of $x^{p^n} - x$, the roots of this polynomial form a field; indeed the p^n roots of $x(x^{p^n-1} - 1)$ are all different since $p^n - 1$ is not divisible by p (see 3-12).

Let α and β be roots, then

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta,$$
$$(\alpha : \beta)^{p^n} = \alpha^{p^n} : \beta^{p^n} = \alpha : \beta;$$

moreover since the characteristic is equal to p, it results from the binomial theorem :

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta.$$

Hence $\alpha\,\beta$, $\alpha : \beta$, $\alpha \pm \beta$ are roots of $x^{p^n} - x$. These roots form therefore a field. Hence the following theorem holds.

Theorem 1. To every power p^n of a primenumber p there corresponds a Galoisfield GF_{p^n} which is uniquely determined in the sense of isomorphism. p is the characteristic of the Galoisfield, and $n = [GF_{p^n} : GF_p]$. Every element of GF_{p^n} is a root of the polynomial (3), and the elements $\neq 0$ are powers of any primitive root of $x^{p^n-1} - 1$.

If Γ' is a subfield of GF_{p^n}, its characteristic must be equal to p. Thus $\Gamma' = GF_{p^m}$, where $m = [\Gamma' : GF_p]$ is a divisor of $n = [GF_{p^n} : GF_p]$. The elements $\neq 0$ of Γ' are roots of $x^{p^m-1} - 1$. Now $p^n - 1 = (p^m - 1)\, s$, where $s = 1 + p^m + \dots + p^{n-m}$ as n is divisible by m. Hence $x^{p^n-1} - 1$ is divisible by $(x^{p^m-1} - 1)$. There are therefore exactly $p^m - 1$ roots of $x^{p^m-1} - 1$ in GF_{p^n}. Hence

Theorem 2. If m is a divisor of n, then GF_{p^n} has exactly one subfield of the type GF_{p^m}, and these are the only subfields of GF_{p^n}.

Furthermore :

Theorem 3. Every finite extension of a Galoisfield has a primitive element and is a normal extension.

Proof. Every finite extension of a Galoisfield Γ is again a Galoisfield, say $\Gamma^* = GF_{p^N}$. This field contains primitive roots of $f(x) = x^{p^N-1} - 1$. If α is a primitive root, then $\Gamma^* = \Gamma(\alpha)$, and Γ^* is the smallest extension admitting the complete reduction of $f(x)$; thus Γ^* is a normal extension of Γ. Hence the theorem.

The last theorem complements the theorem of 2-72 about the primitive elements in finite extensions of fields with an infinite number of elements. In that theorem, a supposition about separability of polynomials was made. The reason why no similar supposition occured in the last theorem, will become obvious from the following theorem.

Theorem 4. Every irreducible polynomial of $GF_{p^n}[x]$ is separable.

Proof. Suppose $f(x)$ to be irreducible and non-separable ; then $f(x) = g(x^p) = a_0 + a_1 x^p + \dots + a_m x^{m}$. Since the coefficients $a_0, \dots, a_m$ are elements of GF_{p^n}, so $a_j = a_j^{p^n} = b_j^p$. Hence $f(x) = b_0^p + (b_1 x)^p + (b_m x^m)^p = (b_0 + b_1 x + \ldots + b_m x^m)^p$ is reducible, contrary to the supposition made for $f(x)$.

It may be mentioned especially that though every primitive root $x^{p^n-1} - 1$ is a primitive element of the extension $\Gamma = GF_{p^n}$ over its prime field $K = GF_p$, not every primitive element of the extension is a primitive root. The only condition for an element α of Γ to be a primitive element, is that it must be a root of an irreducible factor of $x^{p^n-1} - 1$ which has the degree n. Then $[K(\alpha) : K] = n = [\Gamma : K]$ and therefore $[\Gamma : K(\alpha)] = 1$, and therefore $\Gamma = K(\alpha)$. This condition can be satisfied by roots of $x^{p^n-1} - 1$ which have a smaller order than $p^n - 1$. For an example, see 3-23.

3-22. *Automorphisms.* To investigate the Galoisfields somewhat closer, consider the automorphisms of them. Every automorphism of a field leaves the nullelement and the unitelement invariant; the same holds for the elements *2*, *3*, ... as these elements are generated by a repeated addition of the unitelement, thus the elements of the primefield of a Galoisfield are not altered by an automorphism. $\Gamma = GF_{p^n}$ is a normal extension of the primefield $K = GF_p$. An automorphism of Γ is therefore (see 2-742) uniquely determined if it is known into which root of the same polynomial any root of an irreducible polynomial of degree n is to be transformed. Hence there exist exactly n automorphisms of GF_{p^n}. These n automorphisms can be constructed in a very simple way.

Theorem 1. Let β run over the p^n elements of GF_{p^n}, then the mapping $\beta \rightarrow \beta^p$ is an automorphism A of GF_{p^n}.

Proof. As in a field of characteristic p, $(\alpha\,\beta)^p = \alpha^p\,\beta^p$, $(\alpha : \beta) = \alpha^p : \beta^p$, $(\alpha \pm \beta)^p = \alpha^p \pm \beta^p$ hold, the operations of addition, subtraction, multiplication and division are invariant. The mapping is therefore invariant, hence it is a homomorphism. The image consists of more than one element; it is therefore a field. A field cannot be homomorphic to a field unless the fields are isomorphic. Hence the image consists of p^n different elements of GF_{p^n}, and therefore of all the elements of GF_{p^n}; thus the mapping is an automorphism.

By repeating the automorphism A one gets another automorphism A^2 mapping β on β^{p^2}, correspondingly $A^3, \ldots, A^n$. The last of these automorphisms maps β on $\beta^{p^n} = \beta$, hence A^n is the identity. A primitive root is transformed by

$$A, \ldots, A^n \tag{1}$$

into different elements. Hence these n automorphisms are all different, and as there exist exactly n automorphisms of GF_{p^n}, the automorphisms (1) form a full set of the automorphisms of GF_{p^n}. Hence the following theorem holds.

Theorem 2. The automorphisms of GF_{p^n} consist of the transformations (1), where A^k maps every element β of GF_{p^n} on β^{p^k}. The elements of the primefield remain invariant for every automorphism.

Corollary. Let $f(x)$ be a polynomial of $GF_p[x]$; if α is a root of $f(x)$, then $\alpha^p, \alpha^{p^2}, \ldots$ are also roots of $f(x)$.

Proof. $GF_p(\alpha)$ is a Galoisfield, say GF_{p^r}. By the automorphism A^k the coefficients of $f(x)$ are invariant; therefore α is transformed into a root of $f(x)$. Hence α^{p^k} is a root of $f(x)$.

3·23. *Calculation in a Galoisfield.* To show how calculation is done in a Galoisfield, an example will be considered now. The elements of GF_{5^2} are roots of $x^{25} - x = 0$. The cyclotomic polynomial can be calculated by the rules of 3·13; it is $x^8 - x^4 + 1$. This polynomial cannot be irreducible in $GF_5[x]$ since $[FG_{5^2} : GF_5] = 2$, and therefore every element is of order 2 over GF_5. Indeed in GF_5 there is

$$(x^8 - x^4 + 1) = f_1(x)\, f_2(x)\, f_3(x)\, f_4(x), \tag{1}$$

where $f_1(x) = x^2 - x + 2, f_2(x) = x^2 + x + 2, f_3(x) = x^2 + 2x + 3, f_4(x) = x^2 - 2x + 3$. If α is any primitive root of $x^{24} - 1$, then the other primitive roots are $\alpha^5, \alpha^7, c^{11}, \alpha^{13}, \alpha^{17}, \alpha^{19}, \alpha^{23}$, since the exponents must be relatively prime to 24. Furthermore $\alpha^m = \alpha^{24+m}, \alpha^{12} = -1$. From the last corollary it follows that if α^m is a root of $f(x)$, α^{5m} is the second root. Hence the 8 primitive roots consist of the four pairs

$$\alpha,\ \alpha^5;\ \alpha^{13},\ \alpha^{17};\ \alpha^{19},\ \alpha^{23};\ \alpha^7,\ \alpha^{11}. \tag{2}$$

In these 4 pairs, each root is the 5th power of the other one. But one cannot allot the pairs (2) in an arbitrary manner to the 4 irreducible polynomials (1) as their roots. Without loss of generality, suppose that α is a root of $f_1(x)$, then $-\alpha = \alpha^{13}$ is a root of $f_2(x)$. Since α is a root of $f_1(x)$,

$$\alpha^2 = \alpha - 2. \tag{3}$$

$\alpha^3 = \alpha^2 - 2\alpha = -(\alpha + 2)$, $\alpha^6 = \alpha^2 + 4\alpha + 4 = 2$. Hence

$$\alpha^6 = 2 = -3,\ \alpha^{12} = 4 = -1,\ \alpha^{18} = 3 = -2,\ \alpha^{24} = 1 = -4. \tag{4}$$

Therefore $\alpha^7 = 2\alpha$, $\alpha^{14} = -\alpha^2 = 2 - \alpha$. Hence α^7 is a root of $f_4(x)$. Thus the 4 pairs of roots (2) correspond to the 4 polynomials (1) in the order as given there.

$$1, \ \alpha \tag{5}$$

form a basis of GF_{5^2} over GF_5. Thus one can express every element in the form

$$a + b\,\alpha, \tag{6}$$

where a and b are elements of GF_5, *i.e.* integral numbers mod. 5. The multiplication of two elements (6) can be effected by

$$(a + b\,\alpha)\,(a' + b'\,\alpha) = a'' + b''\,\alpha,$$

where, as a consequence of (3),

$$\begin{aligned} a'' &= aa' + 3bb' \\ b'' &= ba' + (a + b)b'. \end{aligned} \tag{7}$$

From (7) one gets $a' + b'\,\alpha = (a'' + b''\,\alpha) : (a + b\alpha)$, where

$$\begin{aligned} a' &= [(a + b)a'' + 2bb''] : (a^2 + ab + 2b^2) \\ b' &= [4ba'' \qquad + \ ab''] : (a^2 + ab + 2b^2). \end{aligned} \tag{8}$$

Since in a field the division by every element $\neq 0$ can be performed, one must expect that for elements a,b of GF_5, the divisor on the right hand side of (8) cannot be 0 unless $a = b = 0$. Of course for $b = 0$ the divisor cannot be equal to 0 unless $a = 0$. For $b \neq 0$, put $a : b = x$; then $x^2 + x + 2 = f_2(x)$ [see (1)] is irreducible; hence there exists no $a : b = x$ in GF_5 by which the equation $x^2 + x + 2 = 0$ could be satisfied. By the help of (7) and (8), the multiplication and the division of any pair of elements (6) of GF_{5^2} can be performed, but the method is not very convenient.

To make the calculations easier, one may express $\alpha, \ldots, \alpha^{24}$ by the help of the basis (5).

$$\begin{array}{llll}
\alpha = \alpha & \alpha^7 = 2\alpha & \alpha^{13} = 4\alpha & \alpha^{19} = 3\alpha \\
\alpha^2 = 3 + \alpha & \alpha^8 = 1 + 2\alpha & \alpha^{14} = 2 + 4\alpha & \alpha^{20} = 4 + 3\alpha \\
\alpha^3 = 3 + 4\alpha & \alpha^9 = 1 + 3\alpha & \alpha^{15} = 2 + \alpha & \alpha^{21} = 4 + 2\alpha \\
\alpha^4 = 2 + 2\alpha & \alpha^{10} = 4 + 4\alpha & \alpha^{16} = 3 + 3\alpha & \alpha^{22} = 1 + \alpha \\
\alpha^5 = 1 + 4\alpha & \alpha^{11} = 2 + 3\alpha & \alpha^{17} = 4 + \alpha & \alpha^{23} = 3 + 2\alpha \\
\alpha^6 = 2 & \alpha^{12} = 4 & \alpha^{18} = 3 & \alpha^{24} = 1.
\end{array} \tag{9}$$

In this table, one gets every column from the preceding one by multiplying with $\alpha^6 = 2$, thus very little calculation only was necessary. It is convenient to supplement (9) by a second table, wherefrom the exponent m of $\alpha^m = a + b\alpha$ is seen when a and b are known. The rows in the following table give the values of a, the columns give the values of b.

	b = 0	1	2	3	4
$a = 0$		1	7	19	13
1	24	22	8	9	5
2	6	15	4	11	14
3	18	2	23	16	3
4	12	17	21	20	10 .

(10)

E.g. To calculate $(2 + 3\alpha)\,(4 + 2\alpha)$, one finds in (10) that the exponents of the two factors are 11 and 21, the product is therefore equal to α^8, and from (9) one sees that $\alpha^8 = 1 + 2\alpha$. In other examples, one has to proceed in a similar way. When the primenumber p is very large, it is convenient to provide for a special table for the multiplication in the primefield GF_p; the arrangement of the "log-tables" (9) and (10) must be made according to the special needs of the problem concerned.

3·24. *Application on the theory of numbers.* The theory of the Galoisfield is very closely connected with the elementary theory of numbers. Some arithmetical propositions are immediate consequences of properties of the primefields GF_p. Equality of two elements of GF_p means that the corresponding integral numbers are congruent (mod.p). As in GF_p, every element is a root of $x^{p-1} - 1$, it follows for integral numbers :

Fermat's theorem :

$$n^{p-1} \equiv 1 \text{ (mod.p), for n not divisible by p.} \tag{1}$$

To every element $\alpha \neq 0$ in GF_{p^n}, there exists an inverse element β such that $\alpha\,\beta = 1$; only 1 and -1 are roots of $x^2 = 1$, and therefore self-inverse, the other elements $\neq 0$ are divided into pairs of inverse elements.

Hence the product of all numbers $\neq 0$ of GF_{p^n} is -1.

For n = 1, it follows *Wilson's* theorem :

$$(p-1)\,! \equiv -1 \text{ (mod.p).} \tag{2}$$

Let p be $\neq 2$, $p^n - 1 = 2m$. As $x^{p^n} - 1 = (x^m - 1)(x^m + 1)$, there are 2 classes of elements $\neq 0$ in GF_{p^n}, the m^{th} power of the elements of the first class is $+ 1$, and the m^{th} power of those of the second is $- 1$. If α is a primitive element of GF_{p^n}, the numbers $\alpha, \ldots, \alpha^{2m} = 1$ are all different, hence $\alpha^m = -1$, and therefore the odd powers of α^m are -1, the even powers are $+ 1$. If $\beta = \gamma^2$, then $\beta^m = (\gamma^m)^2 = (\pm 1)^2 = 1$. Hence every square is an element of the first kind, and every element of the first kind is an even power of α and therefore a square. The product of two elements of a different kind is of the second kind and the product of two elements of the same kind is of the first kind. The element $- 1$ is of the first kind if $(-1)^m - 1 = 0$, *i.e.* if m is even, and it is of the second kind if m is odd.

In GF_p, to every element γ, there corresponds a class (c) of elements congruent c (mod. p), and α is a square in GF_p if and only if $x^2 \equiv \gamma$ (mod. p) has solutions. In this case γ is said to be a *quadratic residue of* p ; if there is no solution, γ is a *quadratic non-residue*. Hence there are $\frac{1}{2}(p - 1)$ quadratic residues and $\frac{1}{2}(p - 1)$ quadratic non-residues. The product of two residues (two non-residues) is a residue ; the product of a residue and non-residue is a non-residue.

Again put $p = 2m + 1$; then the element $- 1$ of GF_p is a square if and only if it is a root of $x^m - 1$, *i.e.* if m is even, say $m = 2n$. Hence

$$\left.\begin{array}{l} -1 \text{ is a quadratic residue of the primenumbers } 4n + 1, \\ -1 \text{ is a quadratic non-residue of the primenumbers } 4n - 1. \end{array}\right\} \quad (3)$$

The primitive roots of $x^{p^n} - 1$ are the roots of the cyclotomic polynomial which is of degree $\phi(p^n - 1)$. In GF_{p^n}, each of these roots is a root of a polynomial of degree n which is irreducible in GF_p, since a primitive root is a primitive element of GF_{p^n} when this field is considered as an extension of its primefield. The cyclotomic polynomial is therefore a product of polynomials which are irreducible in GF_p and each of degree n.

Hence : $\phi(p^n - 1)$ *is divisible by* n *when* p *is a primenumber.*

*3·25. *Application on finite geometries.* Galoisfields have been used to construct finite geometries. Consider e.g. plane projective geometry. Its fundamental notions are : *point, straight line* and the relation of *incidence*. Analytically, the points as well as the straight lines are represented as classes of triplets of real numbers ; two triplets belong to the same class if they differ only by a common factor $\neq 0$; the triplet (0, 0, 0) must be omitted. Thus one considers points $P = \rho(x_1, x_2, x_3)$ and straight lines $g = \sigma[u_1, u_2, u_3]$;

the condition of incidence is

$$x_1 u_1 + x_2 u_2 + x_3 u_3 = 0.$$

For a certain portion of plane projective geometry, it is not important that the numbers ρ, σ, x_i, u_j are real; they may be complex or they may be elements of any particular field. If one selects a Galoisfield for this purpose, one gets a *Veblen geometry*, and the number of points and straight lines is finite.

The simplest case corresponds to GF_2. Here 0 and 1 are the only elements. The arbitrary factors $\rho \neq 0$ and $\sigma \neq 0$ are equal to 1 and can therefore be omitted. This geometry consists of 7 points and 7 straight lines.

$A = (0, 0, 1)$, $B = (0, 1, 0)$, $C = (0, 1, 1)$, $D = (1, 0, 0)$, $E = (1, 0, 1)$,
$F = (1, 1, 0)$, $G = (1, 1, 1)$;

$a = [0, 0, 1]$, $b = [0, 1, 0]$, $c = [0, 1, 1]$, $d = [1, 0, 0]$, $e = [1, 0, 1]$,
$f = [1, 1, 0]$, $g = [1, 1, 1]$.

Every straight line is incident with 3 points, and these are distributed on the straight lines as follows:

a: B D F
b: A D E
c: C D G
d: A B C
e: B E G
f: A F G
g: C E F.

In a similar way, one gets more complicated Veblen geometries by using any kind of Galoisfield to build up a projective, or an affine geometry in n dimensions.

3·251. *Application on statistical analysis.* Consider now the above scheme without any respect to its geometrical significance nor to the algebraic method by which it has been attained. It consists of $v = 7$ *varieties* A, B, C, D, E, F, G, each being repeated $r = 3$ times in the scheme. The varieties are arranged into $b = 7$ *blocks* each consisting of $k = 3$ different varieties. Each of the $v(v-1) : 2$ pairs of varieties occurs in $\lambda = 1$ blocks. Schemes of this kind (for various numbers v, b, r, k, λ) are called in Statistics *balanced incomplete block designs*, and they seem to be very important for the design of agricultural experiments amenable to exact statistical analysis. In the last few years the Galoisfields and the methods of finite geometry have been used successfully for the construction of those designs. It is a startling idea that Galoisfields might be helpful to provide people with more and better food.

3·3. *The fields* K(i).

3·31. *The general case.* Given a field K, where

$$x^2 + 1 \tag{1}$$

is irreducible ; consider the extension K(i) of K, when i is a root of (1). At first, let K be of characteristic p. In GF_2, $x^2 + 1 = (x + 1)^2$, and for $p = 4n + 1$, the polynomial (1) is reducible since -1 is a quadratic residue of p(see 3·24) ; hence $p = 4n + 3$. K may also be of characteristic 0 ; indeed (1) is irreducible in every field which consists of real numbers, and in isomorphic fields. If a and b are elements of K,

then $$a^2 + b^2 = 0, \text{ implies } a = b = 0, \tag{2}$$

since for $b \neq 0$, the element $a : b$ of K must be a root of (1). The field K(i) is isomorphic to the field formed by the classes of residues of the polynomial (1) in the ring K[x] . *A. L. Cauchy* introduced the complex numbers in this manner choosing K as the field of the real numbers. The elements

$$1,\ i \tag{3}$$

form a basis of K(i). Thus the elements are all represented by

$$a + b\,i, \tag{4}$$

where a, b run over all the elements of K. The multiplication formula is

$$(a + bi)\ (a' + b'i) = a'' + b''i,$$

where

$$a'' = a\,a' - b\,b',\ \ b'' = ab' + ba'. \tag{5}$$

The division-formula is therefore

$$(a'' + b''i)\ :\ (a + bi)\ =\ a' + b'i,$$

where

$$a' = (a\,a'' + b\,b'')\ :\ (a^2 + b^2)$$

$$b' = (a\,b'' - b\,a'')\ :\ (a^2 + b^2). \tag{6}$$

Independent of the general theory given before, one can define the field K(i) in the following manner: "Given a field K, satisfying (2); then pairs a,b of elements of K form a vectorspace of elements which are denoted by (4). Determine now the multiplication of the vectors by (5), and in consequence of it, the division by (6), then the vectorspace is made a field in which $0 + 1\,i$ and $0 - 1\,i$ are the roots of $x^2 + 1$." It is left to the reader to check this statement in all its details. Put the field of the real numbers for K, then one gets the most usual way of introducing complex numbers into analysis. By interpreting the vectorspace of rank 2, formed by the elements (4) as an Euclidean space, one comes to the ordinary geometrical representation of the complex numbers.

In K(i)[x], there is $(x^2 + 1) = (x + i)\,(x - i)$. The field K($i$) is a normal extension of K, and i is a primitive element. From 2-742 it follows that the extension admits only one automorphism A which is different from the identity, and that A interchanges the elements $+ i$ and $- i$. Elements which are interchanged by A are said to be *conjugate*; and the conjugate of an element α is denoted by $\overline{\alpha}$. Hence

$$\alpha = a + b\,i \quad \text{implies} \quad \overline{\alpha} = a - b\,i. \tag{7}$$

Hence an element is selfconjugate if and only if it belongs to K. The product of 2 conjugate elements is selfconjugate and is said to be the *norm* N of those elements. Using the notation (7) one gets therefore

$$\alpha\,\overline{\alpha} = N(\alpha) = N(\overline{\alpha}) = a^2 + b^2. \tag{8}$$

From (2) and (8) it follows therefore that $N(\alpha) = 0$ implies $\alpha = 0$. Furthermore

$$N(\alpha\beta) = N(\alpha)\,N(\beta), \quad N(\alpha : \beta) = N(\alpha) : N(\beta),$$

and for elements a of K, there is $N(a) = a^2$.

3-32. *The field $R(i)$.* Consider in particular the field $R(i)$, where R denotes the field of the *rational numbers*. The elements of $R(i)$ can be represented by $(a + bi) : c$, where a,b,c are integral numbers. Hence $R(i)$ is the quotientfield of the integral domain S which consists of all the elements $a + bi$, where a and b are integers. If $\alpha \neq 0$ is an element of S, then $N(\alpha)$ is a positive integral number; if in particular α is a unity of S, then $N(\alpha)$ and $N(1 : \alpha) = 1 : N(\alpha)$ must be positive integral numbers, and therefore $N(\alpha) = a^2 + b^2 = 1$ holds. Hence $1, -1, i, -i$ are the only unities of S, and at the same time the only elements of S for which the norm is equal to 1.

Theorem 1. S is a Euclidean domain.

Proof. It suffices to show that for the elements α of S, the function $N(\alpha)$ has the properties of a norm-function as required in 2·42 and 2·44. Indeed for every $\alpha \neq 0$, the norm $N(\alpha)$ is a positive integral number, and from $N(\alpha\,\beta) = N(\alpha)\ N(\beta)$ it follows, that $N(\alpha\,\beta) \geqq N(\alpha)$, where equality holds if and only if β is a unity; hence the conditions of 2·42 are satisfied. It remains to prove (see 2·44) that to every pair $\alpha_1 \neq 0$, $\alpha_2 \neq 0$, of elements of S there exist such elements β and α_3 that

$$\alpha_1 + \beta\alpha_2 = \alpha_3, \quad \text{where } N(\alpha_2) > N(\alpha_3).$$

To prove this proposition, consider the element $\omega = \alpha_1 : \alpha_2 = r + si$ of $R(i)$. The rational numbers r and s can be represented by $r = a + r'$, $s = b + s'$, where a and b are integers and $|r'| \leqq \frac{1}{2}$, $|s'| \leqq \frac{1}{2}$. Hence $\omega = \beta + \omega'$, where β is an element of S and $N(\omega') = r'^2 + s'^2 \leqq \frac{1}{2}$. By multiplying with α_2 it follows $\alpha_1 = \beta\ \alpha_2 + \omega'\ \alpha_2$. But $\omega'\ \alpha_2 = \alpha_1 - \beta\alpha_2$ must be an element of S, say α_3 and $N(\alpha_3) = N(\alpha_2)\ N(\omega') \leqq \frac{1}{2}\ N(\alpha_2) < N(\alpha_2)$. Hence the theorem.

Corollary. In S the factorisation is unique, and for every two elements, there exists an *h. c. f.* which can be determined by the algorithmus of the *h. c. f.*

Proof. It has been shown in 2·44, theorem 2 that this property holds in every Euclidean domain.

S contains the domain I of the integral numbers as a subring. It is interesting to compare the factorisation in S with the factorisation in I. Every rational number contained in S is an integral number. Hence if an integral number a is divisible in S by an integral number b, then $a : b$ is integral, and therefore a is divisible by b also in I. If an integral number is divisible by an element α of S, it is also divisible by $\bar{\alpha}$ as the divisiblity is invariant for the automorphism A. If β is a factor of α, then $N(\beta)$ is a factor of $N(\alpha)$. Hence if $N(\alpha) = p$ is a primenumber, α is a prime-element of S. Let now π by any prime-element of S, and let $N(\pi) = \pi\,\bar{\pi}$ be divisible by a primenumber p, then p must be divisible by π or by its conjugate and therefore by both of them. Hence either the two elements are associated to p and therefore $\pi = i^{\nu}\ p$ (where $\nu = 0, 1, 2, 3$), or $N(\pi) = p$. A prime-element of S is therefore either associated to a primenumber or it is generated by splitting a primenumber into two conjugate prime-factors. Consider the three cases :

(1) $p = 2 = i(1 - i)^2$. The primenumber 2 is associated to the square of $1 - i$; this element of S is a prime-element as $N(1 - i) = 2$ is a primenumber.

(2) A primenumber of the type $4n + 3$ cannot be reprensented as a norm of an element of S as $N(\alpha) = a^2 + b^2 \neq 3(\text{mod.}4)$. Hence these primenumbers cannot be split up into two conjugate prime-factors ; hence they are prime-elements of S.

(3) The primenumbers $p = 4n + 1$ are products of two non-associated prime-elements.

Proof. As it has been shown in 3-24, the number -1 is a quadratic residue of p. Hence there exists an integer d such that $d^2 + 1 = pm$. On the other hand $d^2 + 1 = (d + i)(d - i)$, but none of the factors on the right hand side is divisible by p ; hence p cannot be a prime-element of S ; it is therefore a product $(a + bi)(a - bi)$ of conjugate prime-elements. If these elements would be associates, they could differ by a factor ± 1 or $\pm i$ only. This is possible only if either $a = 0$, or $b = 0$, or $|a| = |b|$. Since p is supposed to be a primenumber of the type $4n + 1$, these cases cannot occur, and p is a product of two non-associate prime-elements of S.

If the primenumbers p_1 and p_2 have a common primefactor π, then its conjugate is also a common prime-factor of them and $p_1 = p_2$ holds. The factorisation of the primenumbers into prime-elements of S is therefore determined by the following theorem.

Theorem 2. The primenumbers of type $4n + 3$ are prime-elements of S ; the primenumber 2 is associate to the square of the prime-element $1 - i$; the primenumbers $p_i = 4\,n_i + 1$ are equal to products of conjugate and non-associate prime-elements. All these prime-elements are different and non-associate, and every prime-element of S is associate to one of them.

Denoting the primenumbers of type $4n + 3$ by $q_1, q_2, \ldots$ and the prime-elements $a + b\,i$ by $\pi_1, \pi_2, \ldots$, the elements $\neq 0$ of S can therefore be represented by

$$\alpha = i^{r'}(1 - i)^{r}\, q_{n_1} \ldots q_{n_s}\, \pi_{m_1} \ldots \pi_{m_t}. \tag{1}$$

Hence

$$N(\alpha) = \alpha\,\bar{\alpha} = 2^{r}\, q_{n_1}{}^{2} \ldots q_{n_s}{}^{2}\, p_{m_1} \ldots p_{m_t}, \tag{2}$$

where the p's are primenumbers of the type $4n + 1$ and products of two conjugate prime-elements. Obviously every product (2) (where neither the q's nor p's are necessarily different one from another) can be considered as a product of two conjugate elements $\alpha\bar{\alpha}$. An integral number is therefore the norm of an element $\neq 0$ of S if and only if it can be represented by (2). On the other hand the necessary and sufficient condition for a norm is that it is the sum of two squares. Thus the considerations about the ring S lead to the following theorem on integral numbers.

Theorem 3. A positive integral number c can be represented as the sum of two squares if and only if in the representation of c as a product of powers of different primenumbers, the primenumbers of type $4n + 3$ occur with even exponents only.

3-33. *A generalisation.* If K is the field of the real numbers, and α runs over $K(i)$, then $N(\alpha)$ runs over the non-negative real numbers. The sum of two norms $N(\alpha) + N(\beta)$ is again* a "norm" and is different from 0, unless $\alpha = \beta = 0$. This case admits an interesting generalisation which concerns a special case of what has been considered at the end of 2-742.

Suppose that K and Λ are two fields such that $[\Lambda : K] = 2$, and that to every pair of elements $(\alpha, \alpha') \neq (0, 0)$ of Λ, there exists an element $\alpha'' \neq 0$ satisfying

$$\alpha\,\bar{\alpha} + \alpha'\,\bar{\alpha}' = \alpha''\,\bar{\alpha}''. \tag{1}$$

Let $\alpha_1, \alpha_2, \alpha_3$ be different from $0, 0, 0$. Without loss of generality suppose $\alpha_1 \neq 0$. Then $(\alpha_1\,\bar{\alpha}_1 + \alpha_2\,\bar{\alpha}_2) + \alpha_3\,\bar{\alpha}_3 = \alpha_4\,\bar{\alpha}_4 + \alpha_3\,\bar{\alpha}_3 = \alpha\,\bar{\alpha}$, where α_4 and therefore α are different from 0. By repetition of this procedure one gets :

Theorem 1. If K and Λ have the properties as supposed here, for every n-tuplet $\alpha_1, \ldots, \alpha_n \neq 0, \ldots, 0$ of elements of Λ there is

$$\alpha_1\,\bar{\alpha}_1 + \ldots + \alpha_n\,\bar{\alpha}_n = \alpha\bar{\alpha} \neq 0. \tag{2}$$

For elements $a_1, \ldots, a_n$ of K, it follows from (2) :

$$a_1^2 + \ldots + a_n^2 = k^2 \neq 0. \tag{2'}$$

By putting $a_1 = \ldots = a_n = 1$, one sees that the characteristic of K must be 0. Moreover $\alpha_1\,\bar{\alpha}_1 + \ldots + \alpha_n\,\bar{\alpha}_n + 1^2 \neq 0$, and therefore the left sides of (2) and (2') are always $\neq -1$. This shows that the field K cannot be chosen arbitrarily. The following theorem is important for the theory of matrices (see 6-5) :

Theorem 2. If K and Λ have the properties as supposed here, and $v^1_1, \ldots, v^1_n \neq 0, \ldots, 0$, are elements of Λ, then there exist in Λ, n^2 elements

---

* $N(\alpha) = \alpha\,\bar{\alpha}$ as in 3-32, but since it is not always an integral number, it is not a norm function (see 2-42 and 2-44) ; for this reason "norm" is put in inverted commas.

u^i_k and an element α_i satisfying the conditions $\sum\limits_k u^i_k \bar{u}^j_k = 0$, for $i \neq j$, $\sum\limits_k u^i_k \bar{u}^i_k = 1$, $\alpha_i u^i_k = v^i_k$ $(k = 1, \ldots, n)$.

Proof. Let $\bar{v}^2_1, \ldots, \bar{v}^2_n$ be any solution of $\sum v^1_k x_k = 0$; if $n > 2$, then the two equations $\sum v^1_k x_k = 0$, $\sum v^2_k x_k = 0$ again admit solutions; let $\bar{v}^3_1, \ldots, \bar{v}^3_n$ be one of them. Continuing in this manner, one gets n^2 elements v^i_k for which $\sum\limits_k \bar{v}^i_k v^j_k = 0$, for $i \neq j$ holds. Now $\sum\limits_k \bar{v}^i_k v^i_k = \alpha_i \bar{\alpha}_i \neq 0$. Hence $u^i_k = v^i_k : \alpha_i$ is a system with the required properties.

Exercises. 1. The elements $\alpha \bar{\alpha} - \alpha' \bar{\alpha}'$ form a field.

2. This field is identical with K.

3. If every "norm" $\alpha\bar{\alpha}$ is equal to the "norm" a^2 of an element of K, then $\Lambda = K(i)$.

3·4. *Irreducibility of polynomials.*

In nearly every application of the methods of general algebra to a particular problem, one is faced with the task to establish the irreducibility of a polynomial. As irreducibility depends on the coefficients of the polynomial as well as on the field for which it should be proved, the problem needs particular investigations for the single cases. Criteria have been developed especially for the field of the rational numbers. Some of the principles used there can be generalised for a larger class of fields.

*3·41. *A general method.* Consider at first a method which, though applicable to every field, is nevertheless of little practical use. A polynomial $f(x)$ of degree n will be shown to be irreducible in $K[x]$ if and only if a homogeneous equation of the nth degree, $F(x_1, \ldots, x_n) = 0$ has no solution $\alpha_1, \ldots, \alpha_n$ in K. The coefficients of F belong to the ring generated by the coefficients of $f(x)$, and they can be calculated by elementary methods. However it is in general not easier to show that $F(x_1, \ldots, x_n)$ has no solution in K, than to establish the irreducibility of $f(x)$. On the contrary, the irreducibility of $f(x)$, when proved, helps to show that F has no solution in K. The investigation runs as follows.

The classes of residues of a polynomial $f(x)$ in $K[x]$ form a ring which is a field if and only if $f(x)$ is irreducible in $K[x]$ (see 2·47). Let $f(x)$ be of degree n, and α be a root of $f(x)$; $\alpha^n, \alpha^{n+1}, \ldots$ can be linearly expressed by $1, \alpha, \ldots, \alpha^{n-1}$, the coefficients being dependent on those of $f(x)$ only. Hence

$$(x_1 \alpha + \ldots + x_{n-1} \alpha^{n-1} + x_n)(y_1 \alpha + \ldots + y_{n-1} \alpha^{n-1} + y_n) = z_1 \alpha + \ldots + z_{n-1} \alpha^{n-1} + z_n, \quad (1)$$

---

* May be ommitted at the first reading.

where

$$z_j = \sum_{i,k} a^j_{ik}\, x_i\, y_k \text{ for } j = 1, \ldots, n,$$

and a^j_{ik} are elements of K.

The elements $1, \alpha, \ldots, \alpha^{n-1}$ form a basis of a field $K(\alpha)$ with (1) determining the multiplication if and only if to every pair of systems $(x_1, \ldots, x_n)$ and $(z_1, \ldots, z_n)$ of elements of K there exists a uniquely determined system $(y_1, \ldots, y_n)$. Hence the equations

$$y_1\, d^j_1 + \ldots + y_n\, d^j_n = z_j, \text{ where } d^j_k = \sum_i a^j_{ik}\, x_i$$

must have a uniquely determined solution. The necessary and sufficient condition is det $(d^j_k) \neq 0$. But the left hand side of this inequality is an homogeneous polynomial F of degree n in $x_1, \ldots, x_n$. Hence

$$F(x_1, \ldots, x_n) \neq 0, \tag{2}$$

for every system $(x_1, \ldots, x_n)$ of elements of K is the necessary and sufficient condition for $f(x)$ to be irreducible in $K(x)$.

Exercise. To every polynomial $x^3 + px + q$ which is irreducible in $R[x]$ there corresponds a curve of the third class $\sum a_{ijk}\, u_i\, u_j\, u_k = 0$ such that none of its tangents (u_1, u_2, u_3) passes through more than one point with rational coordinates. Compute a_{ijk}.

3-42. *Reduction of the problem to the investigation of irreducibility in $D[x]$.* In many cases it is possible to replace an investigation on irreducibility in $K[x]$ by an investigation on reducibility in $D[x]$, where D is an integral domain. This reduction of the problem to an easier one is based on the following lemma.

Lemma. Let D be an integral domain with unique factorisation, $K = Q(D)$ the quotient-field of D, $f(x)$ and $\varphi(x)$ polynomials of $D[x]$, and $f(x)$ be a primitive polynomial; if $f(x)$ is a factor of $\varphi(x)$ in $K[x]$, then it is also a factor of $\varphi(x)$ in $D[x]$; if $f(x)$ is irreducible in $D[x]$ it is also irreducible in $K[x]$.

Proof. Let $\varphi(x) = f(x)\,\psi(x)$, where $\psi(x)$ is a polynomial of $K[x]$ and $f(x)$ is primitive in $D[x]$ (*i.e.* the common factors of its coefficients are unities of D only); then there exists an element a of D such that $a\psi(x)$ belongs to $D[x]$. Hence $a\varphi(x)$ is divisible by $f(x)$ in $D[x]$. From 2-48, corollary it follows that $\varphi(x)$ is divisible by $f(x)$ in $D[x]$. Let now $\varphi(x)$ be divisible in K[x] by any polynomial $\phi_1(x)$ of degree m, where $0 < \mathrm{m} <$ degree $\phi(x)$. Then $\phi_1(x) = (a : b) f(x)$, where a and b are elements of D, whereas $f(x)$ is a primitive polynomial of $D[x]$ and of degree m. Hence $\phi(x)$ is divisible by $f(x)$ in $D[x]$. Irreducibility in $D[x]$ therefore implies irreducibility in K[x]. Hence the lemma.

3·421. *Irreducibility in $R[x]$.* When the reducibility of a polynomial $\phi(x)$ of $R[x]$ has to be investigated (R, as usual, denotes the field of the rational numbers) one may suppose without loss of generality that the coefficients of $\phi(x)$ are integral numbers. From the preceding lemma it follows that it suffices to inquire whether $\phi(x)$ is reducible in $I[x]$, where I is the ring of the integral numbers. The method described below is applicable in principle to every case as it leads to a decision after a finite number of steps. Its practical application however needs a very skilful handling, otherwise that finite number may become unpracticably large.

Let $\phi(x) = \psi(x)\,\psi_1(x)$, where the coefficients are integral numbers, and $\phi(x)$ is of degree 2n or 2n + 1. Without loss of generality suppose that the degree of $\psi(x)$ is $\leqq$ n. Let $a_0, a_1, \ldots, a_n$ be arbitrary different integers, then $\phi(a_i) = \psi(a_i) . \psi_1(a_i)$; hence $\psi(a_i)$ is a factor of $\phi(a_i)$. Let $\psi(x) = y_0 + y_1 x + \ldots + y_n x^n$, and let $g^1{}_i, \ldots, g^{k_i}{}_i$ be the different factors of $\phi(a_i)$. The integers y must therefore satisfy one of the following systems of n + 1 linear non-homogeneous equations

$$\begin{array}{c} y_0 + a_0\, y_1 + \ldots + a_0{}^n\, y_n = g^{\nu_0}{}_0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ y_0 + a_n\, y_1 + \ldots + a_n{}^n\, y_n = g^{\nu_n}{}_n. \end{array}$$

To every system $\nu_0, \ldots, \nu_n, 0 \leqq \nu_i < \mathrm{k}_i$ there exists a system of equations, and to every system of equations there exists one solution $(y_0, \ldots, y_n)$ as the determinant D_n of the homogeneous systems is $\neq 0$. To prove the last statement one may use mathematical induction. For $\mathrm{n} = 1$, $D_1 = a_1 - a_0 \neq 0$. In the general case, apply the method of sweep-out to the first row by multiplying the first column successively with $a_0, a_0{}^2, \ldots, a_0{}^n$ and subtracting it from the second, third, ... (n + 1)st columns respectively. Hence $D_n = (a_1 - a_0)(a_2 - a_0) \ldots (a_n - a_0) D'$, where

$$D' = \left| \begin{array}{l} 1\ (a_1 + a_0)\ (a_1{}^2 + a_1 a_0 + a_0{}^2) \ldots (a_1{}^{n-1} + a_1{}^{n-2} a_0 + \ldots + a_0{}^{n-1}) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 1\ (a_n + a_0)\ (a_n{}^2 + a_n a_0 + a_0{}^2) \ldots (a_n{}^{n-1} + a_n{}^{n-2} a_0 + \ldots + a_0{}^{n-1}) \end{array} \right| = D_{n-1},$$

as one gets easily by successive column-addition. Thus by mathematical induction it follows that $D_n \neq 0$ (for a different proof, see 3·53). Of the solutions $y_0, \ldots, y_n$, one has to consider only those which consist of integral numbers; finally check by the algorithmus of division whether the polynomials $y_0 + y_1 x + \ldots + y_n x^n$ are factors of $\varphi(x)$, otherwise $\varphi(x)$ is irreducible. This method applies to every integral domain, where the factorisation is unique and there exists a method of factorising any element by a finite number of steps, as can be done in I.

3·43. *Method of homomorphism.* The method of 3·42 becomes more powerful if used in connection with considerations on *homomorphism.* Let

$$\varphi(x) = f(x)\ \psi(x), \tag{1}$$

the three polynomials belonging to $D[x]$. By a suitable homomorphism, D is mapped on an integral domain D_1; the equation (1) is transformed by the same homomorphism into

$$\varphi_1(x) = f_1(x)\ \psi_1(x). \tag{2}$$

Hence if $\varphi_1(x)$ is irreducible, one of its factors, say $\psi_1(x)$, must be associated to a unity of D, and therefore $\varphi(x)$ and $f(x)$ are mapped by the homomorphism on associated polynomials. In this manner, it is often possible to show that irreducibility of $\varphi_1(x)$ in $D_1[x]$ implies the irreducibility of $\phi(x)$ in $D[x]$. Criteria of irreducibility obtained by this method furnish conditions which are sufficient but not necessary for irreducibility, as the reducibility of $\varphi_1(x)$ does not imply the reducibility of $\varphi(x)$. For the application of this method it is essential that D is not a field, as any ring which is homomorphic to a field is isomorphic to it.

3·431. *Eisenstein's theorem.* The method explained in 3·43 will be applied now to prove a theorem from which many more special criteria of irreducibility have been derived. It will be announced here in its original form, though it can easily be generalised to any integral domain with unique factorisation.

Eisenstein's Theorem. Let $a_0, \ldots, a_n$ be integers, $a_0, \ldots, a_{n-1}$ be divisible by an arbitrary primenumber p, a_n be not divisible by p, and a_0 not by p^2, then $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ is irreducible in $R[x]$.

Proof. Represent the domain I of the integral numbers and $I[x]$ by the classes (mod. p). I is mapped homomorphically on a field GF_p and $I[x]$ on $GF_p[x]$ which is a ring with unique factorisation. Let $f(x) = f_1(x)\, f_2(x)$, where degree $f_1(x) = s > 0$ and degree $f(x) = t > 0$. By the homomorphism it follows

$$(f(x)) = (f_1(x))\ (f_2(x)) = (a_n)\ (x) \ldots (x)$$

(where the brackets are used for denoting the classes of residues as in 2-13). As (x) is a prime-element in $D[x]$ and the factorisation in this domain is unique, it follows that

$(f_1(x)) = (c)\,(x)^s,\ (f_2(x)) = (d)\,(x)^t,\ s + t = n$, c and d not divisible by p. Hence

$$f_1(x) = cx^s + p\phi_1(x),\ f_2(x) = dx^t + p\phi_2(x).$$

Hence the term a_n in the product $f_1(x)\,f_2(x)$ is divisible by p^2, contrary to the supposition. Hence $f(x)$ is irreducible in $R[x]$.

3-432. *A special case.* The same homomorphism will be used now to prove the irreducibility of

$$\psi(x) = x^4 + p(ax^3 + bx^2 + cx) + d,$$

where p is a primenumber of the type $4m + 1$, and d is a quadratic non-residue of p. A polynomial of degree < 4 cannot be congruent to $\psi(x)$ mod. p. Hence it suffices to prove that $x^4 + d$ is irreducible in $GF_p[x]$. As -1 is a quadratic residue, there is an integer e such that $(e)^2 = -1$, $(e)^4 = 1$; furthermore $-d$ is a quadratic non-residue. Hence $x^4 + d \equiv 0$ (mod. p) has no solution, and therefore $(x^4 + d)$ has no factor of degree 1 in GF_p. To prove that it has no factor of degree 2, extend GF_p by a root δ of $x^4 + d$. In $GF_p(\delta)$

$$x^4 + d = \prod (x - \delta\, e^r).$$

Each factor of degree 2 has therefore a coefficient $\delta^2\, e^{r+\rho}$. Since δ^2 does not belong to GF_p, $x^4 + d$ is irreducible in GF_p. Hence $\psi(x)$ is irreducible in I and therefore also irreducible in R.

3-433. *Irreducibility of the cyclotomic polynomials in* $R[x]$. The same method has to be applied in a somewhat more subtle manner to prove the irreducibility of the cyclotomic polynomials in $R[x]$.

Theorem. The cyclotomic polynomials are irreducible in the field R of the rational numbers.

Proof. It suffices to prove the irreducibility in $I[x]$ where I is the ring of the integral numbers. Consider $x^n - 1$ as a polynomial in $I[x]$ and let α be a primitive root of it in a suitable extension $R(\alpha)$. Then one gets all the primitive roots in the form α^m where $(m, n) = 1$. Hence one has to prove that if α is a root of a primitive polynomial $f(x)$ which is irreducible in $I[x]$, then α^m is also a root. It suffices to prove it for primenumbers p which are relatively prime to n ; the general case follows from it by a trivial mathematical induction to be taken over the number of the prime-factors of m. As $f(x)$ is a primitive polynomial, it follows from the lemma that it is a factor of $x^n - 1$ in $I[x]$. The coefficient of the highest term is therefore a unity, say

$$f(x) = x^r + a_{r-1}\, x^{r-1} + \ldots + a_0. \tag{1}$$

The elements $1, \alpha, \ldots, \alpha^{r-1}$ form a basis of $R(\alpha)$. The representation of the elements of $R(\alpha)$ by

$$\Sigma\, b_i\, \alpha^i \tag{2}$$

with rational coefficients b_i is therefore unique. $R(\alpha)$ has a submodule M consisting of those elements for which the coefficients b_i are integral numbers. The module M contains

$$\alpha^r = -\, a_{r-1}\, \alpha^{r-1} - \ldots - a_0, \quad \alpha^{r+1} = -\, a_{r-1}\, \alpha^r - \ldots - a_0\, \alpha.$$

Hence M is a ring. As the coefficients of $f(x)$ are integral numbers, $f(x)$ can also be considered as a polynomial in $GF_p[x]$, where p is any primenumber which is relatively prime to n. Let β be a root of $f(x)$ in $GF_p[x]$; so it is a primitive root of $x^n - 1$. Map the ring M on $GF_p(\beta)$ by the correspondence

$$\Sigma\, b_i\, \alpha^i \rightarrow \Sigma\, b_i\, \beta^i, \tag{3}$$

then to every element of M, exactly one element of $GF_p(\beta)$ corresponds. Addition, subtraction and multiplication are invariant for the representation (3); it is therefore a homomorphism. Different elements of M may correspond to the same element of $GF_p(\beta)$ but not conversely. To α^j, for $j = 1, \ldots, n$, there correspond the elements β^j, and as these n elements are all different, no two different elements α^j can correspond to the same power of β. Hence $\alpha, \ldots, \alpha^n$ and $\beta, \ldots, \beta^n$ are put in a (1, 1)— correspondence by (3). The roots of $f(x)$ in $R(\alpha)$ are powers of α, those in $GF_p(\beta)$ are powers of β; as $f(x)$ is unaltered by (3), the exponents must be the same. From the corollary in 3-22 it follows that β^p must be a root of $f(x)$ in $GF_p(\beta)$. Hence α^p is a root of $f(x)$, where p was supposed to be any primenumber which is relatively prime to n. Hence the theorem.

It is remarkable that homomorphisms mapping $R[x]$ on different rings $GF_p[x]$ help to prove the irreducibility of the cyclotomic polynomial in $R[x]$, though the cyclotomic polynomial may be reducible in each of these rings.

Exercise. Show that the cyclotomic polynomial for $n = 8$ is reducible in every GF_p. Discuss the factorisation for the different classes of primenumbers p. Show in particular how the roots are distributed for $p = 3, 5$

and 7, and that from the difference of the distribution of the roots in these three cases, the irreducibility of the polynomial in $R[x]$ already follows.

3·44. *Irreducibility of determinants.* As an example of a proof of irreducibility of a polynomial in more than one indeterminate, the following interesting theorem will be established.

Theorem. Let K be an arbitrary field in which no term in $x^1{}_1, \ldots, x^n{}_n$ occurs, and let $n > 0$, then the determinant $X = \det(x^k{}_i)$ is irreducible in $K[x^1{}_1, \ldots, x^n{}_n]$.

Proof. X is a linear function of each of the n^2 indeterminates, and it is a linear and homogeneous polynomial in the n indeterminates of the first row.

$$X = A_1 x^1{}_1 + \ldots + A_n x^1{}_n.$$

Suppose X to be reducible, then it must be the product of a linear polynomial in $x^1{}_1, \ldots, x^1{}_n$ and a polynomial which is of degree 0 in these indeterminates, the latter being a common factor of $A_1, \ldots, A_n$. If $n > 1$, A_1 is the determinant of the $(n-1)^2$ indeterminates $x^s{}_t$, where $s \neq 1$, $t \neq 1$; if $n = 1$, then $A_1 = 1$. Hence $A_1 \neq 0$, and therefore it is not divisible by any polynomial in indeterminates different from $x^s{}_t$. As there is no indeterminate which occurs in $A_1, A_2, \ldots, A_n$ simultaneously, every common factor of these polynomials must be an element of K. Hence X is irreducible.

3·5. *Symmetric polynomials.*

3·51. *Elementary symmetric polynomials.* Let K be an arbitrary field. A polynomial $f(x_1, \ldots, x_n)$ of $K[x_1, \ldots, x_n]$ is said to be a *symmetric polynomial* if $f(x_1, \ldots, x_n)$ is not altered by any permutation of $x_1, \ldots, x_n$. The integral rational functions corresponding to symmetric polynomials are said to be *integral symmetric functions.*

As the polynomial

$$\prod (x + x_i) = x^n + a_1 x^{n-1} + \ldots + a_n \tag{1}$$

does not change by any permutation of the indeterminates x_i, the coefficients

$$a_i = a_i \ (x_1, \ldots, x_n) \tag{2}$$

are symmetric polynomials. These are called the *elementary symmetric polynomials.* They are represented by

$$
\begin{aligned}
a_1 &= \Sigma\, x_k = x_1 + \dots + x_n \\
a_2 &= \Sigma\, x_{k_1} x_{k_2} \\
&\dots\dots\dots\dots\dots\dots \\
a_i &= \Sigma\, x_{k_1} \dots x_{k_i} \\
&\dots\dots\dots\dots\dots\dots \\
a_n &= \quad x_1 \dots x_n.
\end{aligned}
\tag{3}
$$

The summation has to be taken over all the systems of *different* indices $k_1, \dots, k_i$. Let $f(x) = x^n + b_1 x^{n-1} + \dots + b_n$ be a polynomial of $K[x]$. In a suitable extension of K

$$f(x) = \prod (x - \alpha_k), \tag{4}$$

hence

$$b_i = (-1)^i \; a_i(\alpha_1, \dots, \alpha_n).$$

The coefficients of $f(x)$ are therefore symmetric functions of the roots.

Theorem. Let $f(y_1, \dots, y_n)$ be a polynomial of $K[y_1, \dots, y_n]$, let a_i be the elementary symmetric polynomials, defined by (3), and let $F(x_1, \dots, x_n) = f(a_1, \dots, a_n)$. Then $F(x_1, \dots, x_n)$ is the polynomial 0, only if $f(y_1, \dots, y_n)$ is the polynomial 0.

Proof. Obviously $f(y_1, \dots, y_n) = 0$ implies $F(x_1, \dots, x_n) = 0$. Suppose now that $F(x_1, \dots, x_n) = 0$; it will be shown that $f(y_1, \dots, y_n) = 0$ follows from this supposition. In a suitable extension of $K(y_1, \dots, y_n)$, the polynomial $\phi(z) = z^n - y_1 z^{n-1} + \dots + (-1)^n y_n$ has roots, say $\alpha_1, \dots, \alpha_n$. The elements $y_1, \dots, y_n$ are therefore the elementary symmetric functions of those roots

$$y_i = a_i(\alpha_1, \dots, \alpha_n), \text{ for } i = 1, \dots, n.$$

Put $\alpha_1, \dots, \alpha_n$ for $x_1, \dots, x_n$, then

$$F(\alpha_1, \dots, \alpha_n) = f(y_1, \dots, y_n).$$

As $y_1, \dots, y_n$ are indeterminates over K, the right hand side is different from 0, unless f is the polynomial 0. As however $F(x_1, \dots, x_n) = 0$, so $F(\alpha_1, \dots, \alpha_n) = 0$. Hence the theorem.

Corollary. Let the coefficients of $f(y_1, \dots, y_n)$ be integral numbers and let p be a primenumber. Then $f(a_1, \dots, a_n) = F(x_1, \dots, x_n) \equiv 0$ (mod.p) only if the coefficients of f are congruent to 0 (mod.p).

Proof. The ring $GF_p[x_1, \ldots, x_n]$ is homomorphic to the ring of the polynomials in $x_1, \ldots, x_n$ with integral coefficients. If $F(x_1, \ldots, x_n) \equiv 0$ (mod. p), the corresponding polynomial of $GF_p[x_1, \ldots, x]$ is the polynomial 0, hence $f(y_1, \ldots, y_n)$ corresponds to the polynomial 0 of $GF_p[y_1, \ldots, y_n]$. Therefore the coefficients of f are divisible by p.

3·52. *The main theorem.*

Theorem 1. A symmetric polynomial can be represented in one and only one manner as the sum of homogeneous symmetric polynomials of different degrees.

Proof. Every polynomial of $K[x_1, \ldots, x_n]$ can be represented as the sum of homogeneous polynomials of the same ring, and we can choose the summands so that no two of them have the same degree. The difference of two such representations of the same polynomial is a representation of 0 as a sum of homogeneous polynomials, no two having the same degree, which is impossible. Therefore the representation is unique. A homogeneous polynomial is transformed by a permutation of the indeterminates into a homogeneous polynomial of the same degree; hence the homogeneous portions of a symmetric polynomial are transformed each into itself by every permutation, and they are therefore symmetric homogeneous polynomials.

Let P be a permutation of 1, ..., n, and P' its inverse. If two terms

$$x_{i_1}^{a}, \ldots, x_{i_n}^{c}$$

and $$x_{k_1}^{a}, \ldots, x_{k_n}^{c} \tag{1}$$

with the same system of exponents are transformed by P into equal terms, they will also be transformed by PP' into equal terms and therefore they are equal. Hence by any permutation, different terms are carried into different terms. Therefore the polynomial

$$\Sigma\, x_1^{a} \ldots x_n^{c} \tag{2}$$

which denotes the sum of all *different* terms which one gets by all the permutations of the lower indices of (1) is a symmetric polynomial. By taking the exponents in a non-decreasing order, (2) is represented by the symbol

$$[t_1, \ldots, t_n] = \Sigma\, x_1^{t_n} x_2^{t_n + t_{n-1}} \ldots x_n^{t_n + \cdots + t_1}, \tag{3}$$

where every $t_i \geqq 0$; the summation on the right side of (3) has to be performed as in (2). The degree of $[t_1, \ldots, t_n]$ is

$$m = t_1 + 2t_2 + \ldots + nt_n. \tag{4}$$

Theorem 2. If $f(x_1, \dots, x_n)$ is a homogeneous symmetric polynomial of degree m, it can be represented by

$$f(x_1, \dots, x_n) = \sum_{i=1}^{N} c_i[t_1, \dots, t_n], \tag{5}$$

where c_i are coefficients of f, and the sum is taken over the N different systems of non-negative integers $t_1, \dots, t_n$ satisfying (4).

Proof. As by a suitable permutation of the indeterminates x_i, each term on the right side of (3) can be transformed into every other one and different terms are always transformed into different ones, either each of these terms occurs as a term of f, or none of them does. If therefore one of the terms of (3) has in f the coefficient c_i, then

$$f(x_1, \dots, x_n) - c_i[t_1, \dots, t_n]$$

is a symmetric polynomial in $x_1, \dots, x_n$, where none of the terms of $[t_1, \dots, t_n]$ occurs. By repeating this procedure with all non-negative integral solutions of (4), after N steps, the difference of the two sides of (5) is proved to be equal to 0.

Main theorem of symmetric polynomials. Any symmetric polynomial $f(x_1, \dots, x_n)$ of $K[x_1, \dots, x_n]$ can be represented in one and only one manner by

$$f(x_1, \dots, x_n) = F(a_1, \dots, a_n), \tag{6}$$

where a_i are the elementary symmetric polynomials, and the coefficients of F belong to K.

Proof. The symmetric homogeneous polynomials of degree m form a module M over K(see 2-61) generated by the polynomials $[t_1, \dots, t_n]$. The rank of M is therefore not greater than N. The polynomials

$$a_1^{t_1} \dots a_n^{t_n} \tag{7}$$

belong to M, when the exponents satisfy (4), and from 3-51 it follows that the N polynomials (7) are independent. Hence they form a basis of M. So every homogeneous symmetric polynomial can be represented by (6), and from 3-52 it follows that the same holds for any symmetric polynomial. If there are two such representations by different $F_1(a_1, \dots, a_n)$ and $F_2(a_1, \dots, a_n)$, then the difference must be 0 contrary to 3-51. Hence the main theorem.

Lemma. The polynomials (3) can be generated by addition and subtraction of polynomials (7).

Proof. Let R be the field of the rational numbers. Since every polynomial (3) can be considered as a polynomial of $R[x_1, \ldots, x_n]$, it can be represented as a linear homogeneous function of the N polynomials (7) of the same degree. Therefore an equation

$$c[t_1, \ldots, t_n] = c_1 \prod a_i^{r_i} + \ldots + c_N \prod a_i^{s_i}$$

holds, where $\Sigma r_i = \ldots = \Sigma s_i = m$, and where $c_1, \ldots, c_N$ and $c > 0$ are integers without a common divisor $\neq \pm 1$. It shall be shown that $c = 1$. If not, let p be a prime-factor of c, then not every c_j is divisible by p, and $c_1 \prod a_i^{r_i} + \ldots + c_N \prod a_i^{s_i} \equiv 0$ (mod.p) holds, contrary to the corollary in 3·51. Hence $c = 1$, and the lemma holds.

Since the elements c in (5) are coefficients of $f(x_1, \ldots, x_n)$, the following theorem is a direct consequence of the lemma.

Theorem 3. The coefficients of F are elements of the ring generated by the coefficients of f.

3·53. *Alternating polynomials*. A polynomial $f(x_1, \ldots, x_n)$ of $K[x_1, \ldots, x_n]$ is said to be an *alternating* polynomial if by every odd permutation of $x_1, \ldots, x_n$ it takes the factor -1. As an even permutation is composed of two odd permutations, an alternating polynomial is not altered by any even permutation of the indeterminates. The product of two alternating polynomials is a symmetric polynomial, and the product of an alternating and a symmetric polynomial is alternating. If an alternating polynomial is divisible by an alternating (a symmetric) polynomial, the quotient is a symmetric (an alternating) polynomial. Since every odd permutation is composed of an odd number of transpositions (see 0·3), a polynomial is an alternating one if it takes the factor -1 whenever one transposition of its indeterminates is performed. When the characteristic of K is equal to 2, every alternating polynomial is symmetric and conversely; when the characteristic is different from 2, the polynomial 0 is the only polynomial which can be considered to be symmetric and also to be alternating as well.

Theorem 1. If a polynomial $f(x_1, \ldots, x_n)$ of $K[x_1, \ldots, x_n]$ has the property that by every permutation of the indeterminates it is transformed into a polynomial which is divisible by $f(x_1, \ldots, x_n)$, then it is either symmetric or alternating.

Proof. Let c_{pq} be the factor which is taken by $f(x_1, \ldots, x_n)$ when x_p and x_q are interchanged, then the polynomial takes c_{pq}^2 when this transposition is performed twice; but the twice performed transposition does not alter the polynomial, hence $c_{pq}^2 = 1$. Hence $c_{pq} = \pm 1$. To prove that in this equation the same sign + or − holds for every pair p, q of indices, consider the following identity between transpositions

$$(p, q) = (i, p)\,(k, q)\,(i, k)\,(k, q)\,(i, p).$$

From this equation it follows that

$$c_{pq} = c_{ip}\ c_{kq}\ c_{ik}\ c_{kq}\ c_{ip} = c_{ip}^2\ c_{kq}^2\ c_{ik} = c_{ik}.$$

Hence either every transposition leaves the polynomial invariant, then it is symmetric, or it takes the factor -1 by every transposition, and it is therefore alternating.

Let $f(x_1, \ldots, x_n)$ be an alternating polynomial of $K[x_1, \ldots, x_n]$, where the characteristic of K is different from 2. Replace x_k by x_i, then one gets a polynomial $f(x_1, \ldots, x_i, \ldots, x_i, \ldots, x_n)$ which is alternating, but nevertheless invariant for the interchanging of the ith and the kth indeterminate. Since the characteristic is supposed to be different from 2, the polynomial is 0. Now $f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - f(x_1, \ldots, x_i, \ldots, x_i, \ldots, x_n)$ is divisible by $x_i - x_k$, as one sees by forming the differences of corresponding terms. The n(n−1) : 2 polynomials $x_i - x_k$, where $i < k$, are non-associated prime-elements of $K[x_1, \ldots, x_n]$; hence $f(x_1, \ldots, x_n)$ is divisible by $\prod\limits_{i>k} (x_i - x_k)$. This product is an alternating polynomial itself; the quotient is therefore a symmetric polynomial. Hence the following theorem holds.

Theorem 2. Let $f(x_1, \ldots, x_n)$ be an alternating polynomial of $K[x_1, \ldots, x_n]$, where the characteristic of K is different from 2, and

$$D = \prod_{i>k} (x_i - x_k), \tag{1}$$

then

$$f(x_1, \ldots, x_n) = D\,S, \tag{2}$$

where S is a symmetric polynomial.

Corollary.

$$D = \begin{vmatrix} x_n^{n-1} & \ldots & x_n & 1 \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & \ldots & x_1 & 1 \end{vmatrix}. \tag{3}$$

Proof. The determinant is obviously an alternating polynomial and therefore divisible by D. The second factor S is of degree 0; its value is found to be the unitelement by comparing the coefficient of the diagonal term of the determinant with the coefficient of the corresponding term in D.

3-54. *Symmetric rational functions.*

Theorem 1. Let $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ be polynomials of $K[x_1, \ldots, x_n]$, let $(f, g) = 1$ and $f : g$ be a symmetric rational function, then f and g are symmetric polynomials.

Proof. Let f be transformed into f_1, and g into g_1 by an arbitrary permutation of the indeterminates; then $fg_1 = gf_1$. From 2-47 and the supposition of this theorem it follows that f is divisible by f_1, that g is divisible by g_1 and conversely. As this holds for every permutation of the indeterminates, it follows from the lemma of 3-53 that f and g are symmetric or alternating. If one of them is alternating, the other must also be alternating, for the quotient is symmetric, but in this case the two polynomials must be divisible by D, contrary to the supposition $(f, g) = 1$. Hence f and g are symmetric.

Theorem 2. Let $F(a_1, \ldots, a_n)$ and $G(a_1, \ldots, a_n)$ be polynomials of $K[a_1, \ldots, a_n]$, a_i being the elementary symmetric polynomials of $x_1, \ldots, x_n$, and let $(F, G) = H(a_1, \ldots, a_n)$, $F = f(x_1, \ldots, x_n)$, $G = g(x_1, \ldots, x_n)$, $H = h(x_1, \ldots, x_n)$; then is $h = (f, g)$.

Proof. Let $h' = (f, g)$. From the preceding theorem it follows that $f : h'$ and $g : h'$ are symmetric. Hence h' is symmetric and can be represented by $H'(a_1, \ldots, a_n)$. Since H' is a common factor of F and G, it is divisible by H and therefore h is a factor of h'; but h' is also a factor of h, for $h' = (f, g)$. Hence h and h' are associated, and the theorem holds.

3-55. *Power-sums.* The symmetric polynomials

$$s_k = \sum_{i=1}^{n} x_i^k \tag{1}$$

are called *power-sums*. From (1) it follows for m < n that

$$\begin{aligned} s_1 &= a_1, \\ s_{m-1}\, a_1 &= s_m + \sum x_1^{m-1} x_2 \\ s_{m-k}\, a_k &= \sum x_1^{m-k+1} x_2 \ldots x_k + \sum x_1^{m-k} x_2 \ldots x_{k+1} \\ s_1\, a_{m-1} &= \sum x_1^2 x_2 \ldots x_{m-1} + m a_m. \end{aligned}$$

Hence

$$\sum_{i=1}^{m-1} (-1)^i a_i s_{m-i} = -s_m + (-1)^{m-1} m a_m. \tag{2}$$

Similarly for m > n,

$$\sum_{i=1}^{n} (-1)^i a_i s_{m-i} = -s_m \tag{3}$$

holds.

Theorem. Let K be a field of characteristic 0 ; then a_m can be expressed by $s_1, \ldots, s_m$ with coefficients from K, and therefore the symmetric polynomials of $K[x_1, \ldots, x_n]$ are polynomials of $K[s_1, \ldots, s_n]$.

Proof. $a_1 = s_1$; by mathematical induction we suppose that $a_1, \ldots, a_{m-1}$ can be expressed in terms of $s_1, \ldots, s_{m-1}$. From (2) it follows that a_m can be expressed in terms of $s_1, \ldots, s_m$.

It may be mentioned that this theorem does not hold if K has a characteristic p ≦ n, and that the elementary symmetric polynomials cannot be expressed in terms of power-sums by the help of integral coefficients only. The power-sums offer a possibility to express D^2 in a very simple form, where D is the alternating function defined in 3-53. By squaring the determinant in 3-53, (3) by columnwise multiplication, one gets

$$D^2 = \begin{vmatrix} s_{2n-2} & \ldots & s_n & s_{n-1} \\ s_{2n-3} & \ldots & s_{n-1} & s_{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ s_{n-1} & \ldots & s_1 & n \end{vmatrix} . \tag{4}$$

Exercise. A special problem of the theory of numbers asks for the sets of integral numbers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ satisfying the m conditions

$$\begin{aligned} a_1 + \ldots + a_n &= b_1 + \ldots + b_n \\ a_1^2 + \ldots + a_n^2 &= b_1^2 + \ldots + b_n^2 \\ \cdots\cdots&\cdots\cdots \\ a_1^m + \ldots + a_n^m &= b_n^m + \ldots + b_n^m . \end{aligned}$$

Prove that for m = n there exists no solution except the trivial solutions, where $b_1, \ldots, b_n$ is a permutation of $a_1, \ldots, a_n$.

3-6. *Solution of special equations by radicals.*

Equations of the type

$$x^n - a = 0 \tag{1}$$

are said to be *binomial equations*. If α is a solution of (1), and ε is a primitive root of $x^n - 1$, then the n roots of (1) are given by $\alpha \varepsilon^j$, for j = 1, …, n, and therefore

$$x^n - a = \prod_{j=1}^{n} (x - \alpha \varepsilon^j). \tag{2}$$

Hence $K(\alpha, \varepsilon)$ is the smallest extension of K admitting the complete reduction of $x^n - a$. A solution of (1) is said to be an nth root or nth *radical* of a, or more particularly a square root (cubic root, biquadratic root) when n = 2 (n = 3, n = 4). If a is a positive number, there exists exactly one positive number among the solutions of (1), and in general this solution is meant if one speaks of the radical.[*]

If α_1 is a radical of an element of K, furthermore α_2 is a radical of an element of $K(\alpha_1)$ etc., and α_n is a radical of an element of $K(\alpha_1, \ldots, \alpha_{n-1})$, then every element of $K(\alpha_1, \ldots, \alpha_n)$ can be generated from the elements of K by performing addition, subtraction, multiplication, division *and* extraction of roots. Questions regarding algebraic extensions of this type are answered by Galois' theory of algebraic equations. This theory is intended to be discussed in the second volume. Here, only some special classes of equations which can be solved by radicals will be investigated.

There is little loss of generality in supposing that in the equation

$$x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n = 0 \tag{3}$$

the coefficient b_1 is equal to zero. As $-b_1$ is equal to the sum of the roots, $b_1 = -(\alpha_1 + \ldots + \alpha_n)$. The transformation

$$x' = x + b_1 : n \tag{4}$$

transforms (3) into an equation where the coefficient b_1 is replaced by 0. The transformation (4) can be performed unless n is divisible by the characteristic of the field. For this reason it is supposed for the rest of this section, that the *characteristic of* K *is different from* 2 *and from* 3.

3·61. *Cubic equations.* For n = 2, under the supposition made just beforehand, the general equation can be reduced to $x^2 - a = 0$. This equation can be solved by extracting one square root.

Let n = 3. The reduced form of the equation is

$$f(x) = x^3 + px + q = 0. \tag{1}$$

---

[*] The notion of radical is also used in the theory of ideals and of hypercomplex systems but in a completely different sense.

Let K be a field containing p and q, and let in a suitable extension of K, the roots of (1) be $\alpha_1, \alpha_2, \alpha_3$. The elementary symmetric functions of the roots are therefore

$$a_1 = 0,\ a_2 = p,\ a_3 = -q. \tag{2}$$

By the formulas of 3-54, one computes easily the power-sums as

$$s_1 = 0,\ s_2 = -2p,\ s_3 = -3q,\ s_4 = 2p^2. \tag{3}$$

Put $D = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$. (4)

This alternating function of the roots is called the *discriminant*. Its square is a symmetric function of the roots and therefore it belongs to K. Using the formula for D^2, given in 3-53, one gets

$$D^2 = \begin{vmatrix} s_4 & s_3 & s_2 \\ s_3 & s_2 & s_1 \\ s_2 & s_1 & 3 \end{vmatrix}$$

and putting in the values (3) for the power-sums, it is found that

$$D^2 = -4p^3 - 27q^2. \tag{5}$$

The derivative of $f(x)$ is

$$f'(x) = 3x^2 + p = (x - \alpha_1)(x - \alpha_2) + (x - \alpha_2)(x - \alpha_3) + (x - \alpha_1)(x - \alpha_3).$$

Hence

$$f'(\alpha_1) = 3\,\alpha^2_1 + p = (\alpha_1 - \alpha_2)\ (\alpha_1 - \alpha_3) = D : (\alpha_2 - \alpha_3).$$

Moreover

$$-\alpha_1 = \alpha_2 + \alpha_3.$$

Hence it follows that

$$\alpha_2 = \tfrac{1}{2}[-\alpha_1 + D : (3\alpha_1^2 + p)]$$

and

$$\alpha_3 = \tfrac{1}{2}[-\alpha_1 - D : (3\alpha_1^2 + p)]$$

are elements of $K(D, \alpha_1)$. Since on the other hand D is contained in $K(\alpha_1, \alpha_2, \alpha_3)$,

$$K(D, \alpha_1) = K(\alpha_1, \alpha_2, \alpha_3)$$

holds. Suppose $f(x)$ to be irreducible in $K[x]$. Then α_1 is of degree 3 over K, whereas it follows from (5), that D is of degree 2 or 1 over K. Hence $[K(D, \alpha_1) : K(D)] = 3$.

To get α_1 by extracting square roots and cubic roots only, one needs the roots of the cyclotomic polynomial $x^2 + x + 1$. These are denoted by

$$\omega = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{(-3)} \text{ and } \omega^2 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{(-3)}.$$

Introduce furthermore *Lagrange's* symbols

$$(\omega, \alpha) = \alpha_1 + \omega\,\alpha_2 + \omega^2\,\alpha_3 \text{ and } (\omega^2, \alpha) = \alpha_1 + \omega^2\,\alpha_2 + \omega\,\alpha_3.$$

From $\alpha_1 + \alpha_2 + \alpha_3 = 0$, and $1 + \omega + \omega^2 = 0$, it follows :

$$(\omega, \alpha) + (\omega^2, \alpha) = 3\alpha_1,\ \omega^2(\omega, \alpha) + \omega(\omega^2, \alpha) = 3\alpha_2,\ \omega(\omega, \alpha) + \omega^2(\omega^2, \alpha) = 3\alpha_3. \tag{6}$$

By an elementary calculation, one gets

$$\begin{aligned} (\omega,\ \alpha)^3 &= -\tfrac{27}{2}q + \tfrac{3}{2}D\sqrt{(-3)} \\ (\omega^2,\ \alpha)^3 &= -\tfrac{27}{2}q - \tfrac{3}{2}D\sqrt{(-3)} \end{aligned} \tag{7}$$

$$(\omega, \alpha)\,(\omega^2,\ \alpha) = -3p. \tag{8}$$

From (7) it follows that Lagrange's symbols can be obtained by extracting cubic roots only, after having extracted the square roots of $-4p^3 - 27q^2$ and of -3. By extracting a cubic root a factor ω or ω^2 remains arbitrary. The two arbitrary factors which occur when the cubic roots of the right hand sides in formula (7) are extracted, are interconnected as is seen by (8). If (ω, α) takes a factor ω^ν, then (ω^2, α) takes $\omega^{2\nu}$. These factors generate an even permutation of the roots $\alpha_1, \alpha_2, \alpha_3$. By extracting the square roots of $-4p^3 - 27q^2$ and of -3, a factor ± 1 is left arbitrary. These factors may interchange Lagrange's symbols and generate a transposition of α_2 and α_3. Thus the formulas (5), (6), (7), and (8) determine the three roots uniquely up to an arbitrary permutation of them, and the result is obtained by mere extraction of square roots and cubic roots.

3·62. *Biquadratic equations.* For $n = 4$, the reduced form of the equation is

$$x^4 + p\,x^2 + q\,x + r = 0.$$

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots in a suitable extension of K.

Put

$$\begin{aligned} \beta_1 &= -(\alpha_1 + \alpha_2)\,(\alpha_3 + \alpha_4) \\ \beta_2 &= -(\alpha_1 + \alpha_3)\,(\alpha_2 + \alpha_4) \\ \beta_3 &= -(\alpha_1 + \alpha_4)\,(\alpha_2 + \alpha_3). \end{aligned}$$

Since by a transposition of any two of the roots, the elements $\beta_1, \beta_2, \beta_3$ are interchanged only, by an arbitrary permutation of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ the elements $\beta_1, \beta_2, \beta_3$ are interchanged too, hence any symmetric function of $\beta_1, \beta_2, \beta_3$ is not altered, and it is therefore a symmetric function of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Hence there exists an equation $x^3 + b_1 x^2 + b_2 x + b_3 = 0$ with elements from K having the roots $\beta_1, \beta_2, \beta_3$. Of course, there is

$$b_1 = 2p,\ b_2 = p^2 - 4r,\ b_3 = -q^2.$$

Thus it is possible to find out $\beta_1, \beta_2, \beta_3$ by extracting roots only. In order to find out $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, one has to consider that

$$(\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = 0,\quad (\alpha_1 + \alpha_2)\ (\alpha_3 + \alpha_4) = -\beta_1\ ;$$

hence $\alpha_1 + \alpha_2$ and $\alpha_3 + \alpha_4$ are the roots of $x^2 - \beta_1 = 0$.

$$\alpha_1 + \alpha_2 = \sqrt{\beta_1},\ \alpha_3 + \alpha_4 = -\sqrt{\beta_1}\ ;$$

similarly

$$\alpha_1 + \alpha_3 = \sqrt{\beta_2},\ \alpha_2 + \alpha_4 = -\sqrt{\beta_2},$$

$$\alpha_1 + \alpha_4 = \sqrt{\beta_3},\ \alpha_2 + \alpha_3 = -\sqrt{\beta_3}.$$

For every root, a factor ± 1 remains arbitrary, but since

$$\sqrt{(\beta_1\, \beta_2\, \beta_3)} = (\alpha_1 + \alpha_2)\ (\alpha_1 + \alpha_3)\ (\alpha_1 + \alpha_4)$$

$$= \alpha_1^2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) + \Sigma\, \alpha_i\, \alpha_j\, \alpha_k = -q$$

holds, only two of the factors are arbitrary. The choice of these factors corresponds to a permutation of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ as is seen from the final formulas :

$$2\alpha_1 = \sqrt{\beta_1} + \sqrt{\beta_2} + \sqrt{\beta_3} \quad 2\alpha_3 = -\sqrt{\beta_1} + \sqrt{\beta_2} - \sqrt{\beta_3}$$

$$2\alpha_2 = \sqrt{\beta_1} - \sqrt{\beta_2} - \sqrt{\beta_3} \quad 2\alpha_4 = -\sqrt{\beta_1} - \sqrt{\beta_2} - \sqrt{\beta_3}.$$

If one excludes the cases where K is of characteristic 2 or 3, the equations of degree $\leqq 4$ can therefore be solved by extracting square roots and cubic roots only.

3·7. *Resultants.*

Consider the polynomials

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n,$$

and $$g(x) = x^m + b_1 x^{m-1} + \ldots + b_m, \tag{1}$$

where the coefficients belong to the same field. In a suitably chosen extension, $f(x)$ has the roots $\alpha_1, \ldots, \alpha_n$, and $g(x)$ has the roots $\beta_1, \ldots, \beta_m$. The necessary and sufficient condition for $f(x)$ and $g(x)$ to have a common root, is that the *Resultant*

$$R(f, g) = \prod_{i,k} (\alpha_i - \beta_k) \tag{2}$$

is equal to zero. From (2) it follows immediately :

$$\begin{aligned} R(f, g) &= \prod_i g(\alpha_i) \\ &= (-1)^{mn} R(g, f) \\ &= (-1)^{mn} \prod_k f(\beta_k). \end{aligned} \tag{3}$$

Hence $R(f, g)$ is a polynomial in $\alpha_1, \ldots, \alpha_n$ the coefficients belonging to the ring which is generated by $b_1, \ldots, b_m$; this polynomial is symmetric. From 3·52 it follows therefore that $R(f, g)$ can be expressed by the elementary symmetric polynomials of $\alpha_1, \ldots, \alpha_n$ with coefficients belonging to the ring generated by $b_1, \ldots, b_m$, and since those elementary symmetric polynomials differ from the coefficients of $f(x)$ by factors ± 1 only, the resultant is an element of the ring generated by $a_1, \ldots, a_n, b_1, \ldots, b_m$. Hence

$$R(f, g) = R(1, a_1, \ldots, a_n ; 1, b_1, \ldots, b_m). \tag{4}$$

The reason why the constant 1 is used in this notation will become obvious in 3·72. Suppose that the coefficients of $f(x)$ and $g(x)$ are polynomials of $K[y]$, then $R(f, g)$ is a polynomial of that ring, say $R(f, g) = R(y)$. If $R(y)$ is of degree > 0, there exist in a suitable extension of K, elements $\eta_1, \ldots, \eta_s$ such that $R(\eta_i) = 0$. The polynomials $f(x)$ and $g(x)$ can be considered as elements of the ring $K[x, y]$, say

$$f(x) = f(x, y) ; \; g(x) = g(x, y).$$

Then $f(x, \eta_i)$ and $g(x, \eta_i)$ have common roots ; thus

$$f(\xi, \eta_i) = g(\xi, \eta_i) = 0.$$

In this way, the common solutions of two algebraic equations of two variables

$$f(x, y) = 0, \; g(x, y) = 0$$

can be found by the help of a resultant.

3·71. *Case when the coefficients of the highest term are equal to 1.* To find out $R(f, g)$ in terms of the coefficients a_j and b_k, consider $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ as indeterminates ; the coefficients a_j are symmetric polynomials in the indeterminates α_ν, and similarly the cofficients b_k are symmetric in the indeterminates β_μ. Every term

$$A = a_1^{s_1} \ldots a_n^{s_n} b_1^{t_1} \ldots b_m^{t_m} \tag{1}$$

is a homogeneous polynomial in the n + m indeterminates $\alpha_1, \ldots, \beta_m$ of degree

$$s_1 + 2s_2 + \ldots + n\, s_n + t_1 + \ldots + m\, t_m = w. \tag{2}$$

The integral number w is said to be the *weight* of A. Let $A_1, \ldots, A_N$ be different terms of the type (1) ; then it follows from 3·57 that

$$c_1 A_1 + \ldots + c_N A_N = B \tag{3}$$

cannot be equal to 0 unless the N coefficients c_j are zero each. If the terms A_i are not of the same type and the coefficients a_i are different from zero, B is the sum of homogeneous polynomials in $(\alpha_1, \ldots, \beta_m)$ of different degrees with non-vanishing coefficients, and it is therefore not a homogeneous polynomial. Since $R(f, g)$ is a homogeneous polynomial of degree nm in the indeterminates, it is the sum of terms (1) of the weight nm each. From $R(f, g) = \prod_i g(\alpha_i)$ it is seen that the term $b_m{}^n$ has the coefficient 1 ; furthermore $R(f, g)$ has the property that it is zero when $f(x)$ and $g(x)$ have a common root. It will be proved now that these 3 properties are characteristic for the resultant.

Theorem 1. Let S be the sum of terms (1) of weight nm each with the property that $S = 0$ when $f(x)$ and $g(x)$ have a common root ; moreover let the coefficient of $b_m{}^n$ in S be equal to 1, then $S = R(f, g)$.

Proof. Express S as a polynomial in $\alpha_1, \ldots, \beta_m$; then S can be considered as a polynomial $\psi(\alpha_i)$, the coefficients being polynomials in the remaining n + m − 1 indeterminates. $\psi(\alpha_i) - \psi(\beta_k)$ is divisible by $\alpha_i - \beta_k$. Since S is zero when α_i and β_k are equal, $\psi(\beta_k) = 0$. Hence $S = \psi(\alpha_i)$ is divisible by $\alpha_i - \beta_k$. In the ring generated by the indeterminates $\alpha_1, \ldots, \beta_m$ the factorisation is unique, and the nm irreducible polynomials $\alpha_i - \beta_k$ are non-associate. Now S is divisible by each of them, hence it is divisible by their product which is equal to $R(f, g)$. Since the terms of S are all of weight n m, the quotient must be of weight zero. By supposition, the term $b_m{}^n$ has the coefficient 1 in S, that is the same coefficient as in $R(f, g)$, the quotient is therefore equal to 1. Hence the theorem.

A polynomial in $a_1, \dots, b_m$ with the properties supposed in the last theorem, can be found by the following consideration. If α is a common root of $f(x)$ and $g(x)$, then the following $n + m$ equations hold, and these can be considered as linear homogeneous equations for $\alpha^{n+m}, \alpha^{n+m-1}, \dots, \alpha$.

$$\alpha^m f(\alpha) = 1\, \alpha^{n+m} + \dots + a_n\, \alpha^m + 0\, \alpha^{m-1} + \dots + 0\, \alpha = 0$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\alpha\; f(\alpha) = 0\, \alpha^{n+m} + \dots + 1\, \alpha^{n+1} + a_1\, \alpha^n + \dots + a_n\, \alpha = 0$$

$$\alpha^n g(\alpha) = 1\, \alpha^{n+m} + \dots + b_m\, \alpha^n + 0\, \alpha^{n-1} + \dots 0\, \alpha = 0$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\alpha\; g(\alpha) = 0\, \alpha^{n+m} + \dots\dots\dots + 1\, \alpha^{m+1} + \dots + b_m\; \alpha = 0.$$

$$\begin{vmatrix}
1 & a_1 & \dots & a_n & & & \\
 & 1 & a_1 & \dots & a_n & & \\
\hdotsfor{7} \\
 & & & 1 & a_1 & \dots & a_n \\
1 & b_1 & \dots & b_m & & & \\
 & 1 & b_1 & \dots & b_m & & \\
\hdotsfor{7} \\
 & & & 1 & b_1 & \dots & b_m
\end{vmatrix} = 0, \tag{4}$$

when $f(x)$ and $g(x)$ have a common root. The diagonal element is b_m^n, and this term does not occur any more in the determinant ; hence the term b_m^n in the determinant has the coefficient *1*. The weight of the diagonal element is equal to nm. By interchanging any two columns, the weight of the diagonal-element is either unaltered or the element is equal to zero ; in this manner, one can prove easily that all the terms of the determinant have the same weight; thus the supposition of theorem 1 is satisfied. Hence:

Theorem 2. The determinant (4) is equal to $R(f, g)$.

3·72. *The general case.* Let

$$F(x) = a_0\, x^n + a_1\, x^{n-1} + \dots + a_n \quad \text{and}$$

$$G(x) = b_0\, x^m + b_1\, x^{m-1} + \dots + b_m$$

be polynomials, where the coefficients $a_0, \dots, a_n, b_0, \dots, b_m$ are elements of the same field.

By *definition*, the determinant

$$R(F, G) = \left| \begin{array}{ccccccc} a_0 & a_1 & \dots & a_n & & & \\ & a_0 & a_1 & \dots & a_n & & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & & & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & & b_0 & b_1 & \dots & b_m \end{array} \right| \qquad (1)$$

is called the *resultant of F* and *G*.

For $a_0 = b_0 = 1$, this definition tallies with the definition given for $R(f, g)$ in 3·71; moreover $R(F, G) = (-1)^{mn} R(G, F)$ holds. For any further investigation, one has to distinguish 4 cases.

1. Let $a_0 \neq 0$, $b_0 \neq 0$, $\alpha_1, \dots, \alpha_n$ be the roots of $F(x)$, $\beta_1, \dots, \beta_m$ be the roots of $G(x)$.

Put

$$F(x) : a_0 = f(x) = (x - \alpha_1) \dots (x - \alpha_n)$$

$$G(x) : b_0 = g(x) = (x - \beta_1) \dots (x - \beta_m).$$

Then

$$R(F, G) = a_0^m \, b_0^n \, R(f, g) = a_0^m \, b_0^n \prod_{i, k} (\alpha_i - \beta_k). \qquad (2)$$

Hence $R(f, g) = 0$ is the necessary and sufficient condition for $F(x)$ and $G(x)$ having a common root.

2. Let $a_0 = b_0 = 0$. Then $R(F, G) = 0$, independent of the existence of a common root.

3. $b_0 = b_1 = \dots = b_m = 0$. Then $R(F, G) = 0$; but as every element satisfies the equation $g(x) = 0$, every root of $f(x)$ is a root of $g(x)$. Similarly if $f(x)$ is the polynomial 0.

4. $a_0 \neq 0$, $b_0 = \dots = b_{r-1} = 0$, $b_r \neq 0$. Put $G_r(x) = b_r x^{m-r} + \dots + b_m$, then $R(F, G) = a_0^r R(F, G_r) = a_0^m \, b_r^n \prod_{i, k} (\alpha_i - \beta_k)$; in this case the resultant is equal to zero if and only if there exists a common root. Similarly if $b_0 \neq 0$, $a_0 = \dots = a_{s-1} = 0$, $a_s \neq 0$. Hence:

Theorem. If $F(x)$ and $G(x)$ have a common root, then $R(F, G) = 0$. If on the other hand $R(F, G) = 0$, then $F(x)$ and $G(x)$ have a common root, unless $a_o = b_o = 0$.

It appears that the resultant $R(F, G)$ is not completely determined by the two polynomials $F(x)$ and $G(x)$ themselves, but by the manner how they are represented. In the definition of "polynomial" it was stated (see 2-32) that terms with coefficients zero should not matter, *i.e.* that polynomials differing by such terms are considered to be equal. By adding terms with coefficients zero to $F(x)$ and $G(x)$, one can always arrange that $a_o = b_o = 0$, and therefore $R(F, G) = 0$. This difficulty can be overcome by a rule that polynomials $F(x)$ and $G(x)$ should be written in a standard form where the highest coefficients are different from zero, unless the polynomial is the zero-polynomial. A rule of this kind would however imply another incongruity for the case that the coefficients are functions of a variable, say y; the resultant would cease to be a resultant for such values of y, for which $a_o(y) = 0$ and $b_o(y) = 0$. For this reason, preference has been given to the notation given here. Thus the resultant depends on the manner how the polynomials are represented, and it ceases to be a sufficient condition for a common root as soon as $a_o = b_o = 0$ holds.

Example. To find the solutions of

$$\begin{aligned} y\,x^2 + 2x + y &= 0 \\ y^2 x^2 - 1 \qquad &= 0. \end{aligned}$$

Consider the left hand side as polynomials in x with coeficients from R[y]. The resultant is

$$\begin{vmatrix} y & 2 & y & 0 \\ 0 & y & 2 & y \\ y^2 & 0 & -1 & 0 \\ 0 & y^2 & 0 & -1 \end{vmatrix} = y^2\,(y+1)\,(y-1)\,(y+i\sqrt{3})(y-i\sqrt{3}) = \psi(y).$$

For $y = 0$, there is $a_o = b_o = 0$, and the second equation has no solution. For the four other roots of $\psi(y)$, there is $a_o \neq 0$; $b_o \neq 0$. To each of these roots, there corresponds a solution. These solutions are therefore

$$\begin{array}{llll} y = -1, & y = 1, & y = -i\sqrt{3}, & y = i\sqrt{3}, \\ x = 1; & x = -1; & x = \frac{i}{3}\sqrt{3}; & x = -\frac{i}{3}\sqrt{3}. \end{array}$$

3·73. *Linear representation of a resultant.*

Theorem. Let D be the integral domain generated by the coefficients of $F(x)$ and $G(x)$; then there exist in $D[x]$ polynomials $u(x)$ of degree $< m$, and $v(x)$ of degree $< n$ such that

$$u(x)\ F(x) + v(x)\ G(x) = R(f,\ g). \tag{1}$$

Proof. Consider the $n + m$ equations

$$x^{\mu}\ F(x) = a_0\ x^{n+\mu} + a_1\ x^{n+\mu-1} + \dots + a_n\ x^{\mu},\ \text{for}\ \mu = 0, 1, \dots, m-1$$

$$x^{\nu}\ G(x) = b_0\ x^{m+\nu} + b_1\ x^{m+\nu-1} + \dots + b_m\ x^{\nu},\ \text{for}\ \nu = 0, 1, \dots, n-1.$$

These form a system of linear equations in $x^0, \dots, x^{n+m-1}$; the determinant of the matrix is equal to $R(f, g)$. Multiply each equation with the cofactor of the last element, and add. Then one gets the equation (1), where

$$u(x) = u_1\ x^{m-1} + \dots + u_m,\ v(x) = v_1\ x^{n-1} + \dots + v_n,$$

and $u_1, \dots, v_n$ are the cofactors of the elements of the last column. Hence the theorem.

3-8. *Closed fields.* A field C is said to be *closed* if it is impossible to extend it algebraically, *i.e.* if every polynomial of $C[x]$ of degree > 1 is reducible. The main-result of 3-8 is that the field of all complex numbers is a closed one.

Theorem 1. Let K be a field of characteristic 0. $[\Lambda : K] = 2$; let every polynomial of odd degree of $K[x]$, and also every quadratic polynomial of $\Lambda[x]$ have a root in Λ; then Λ is a closed field.

The proof will be given in two steps. At first it will be shown that any polynomial $\psi(x)$ of $K[x]$ has a root in Λ, and then the same will be proved for the polynomials in $\Lambda[x]$.

Proof. 1. Let $\psi(x)$ be a polynomial of $K[x]$. Without loss of generality, one can suppose that $\psi(x)$ is irreducible; as K is supposed to be of characteristic 0, the polynomial $\psi(x)$ is separable (see 2-65) and its roots in any suitable extension are therefore all different. Let n be the degree of $\psi(x)$ and $n = 2^m u$, where $u \equiv 1 \pmod{2}$, then the proposition holds for $m = 0$; let it be true for $m < k$, and prove it for $m = k > 0$. In a suitable extension, $\psi(x)$ has the roots

$$\alpha_1, \dots, \alpha_n. \tag{1}$$

For an arbitrary element c of K, the number of the elements

$$\alpha_i \alpha_j + c(\alpha_i + \alpha_j), \text{ where i, j} = 1, \ldots, \text{n are different}, \tag{2}$$

is $n(n-1):2$. The ordered pairs of elements $\alpha_i\alpha_j$, $\alpha_i + \alpha_j$ are all different and the non-ordered pairs α_i, α_j are uniquely determined by $\alpha_i \alpha_j$, $\alpha_i + \alpha_j$. As K contains an infinity of elements, one can choose c in such a way that the elements (2) are all different and that

$$\alpha_i \alpha_j + c(\alpha_u + \alpha_v) \neq \alpha_p \alpha_q + c(\alpha_s + \alpha_t), \tag{3}$$

if

$$\alpha_u + \alpha_v \neq \alpha_s + \alpha_t.$$

By an arbitrary permutation of the elements (1), the elements (2) will be interchanged only. Hence every symmetric function of the elements (2) is also a symmetric function of (1) and is therefore an element of K. Thus the elements (2) are the roots of a polynomial $\phi(x)$ of K$[x]$ of degree $n(n-1):2 = 2^{m-1}u(n-1)$. As n is even, $u(n-1)$ is odd; therefore $\phi(x)$ has a root in Λ. Let $\alpha_1 \alpha_2 + c(\alpha_1 + \alpha_2)$ be such a root. $\alpha_1\alpha_2$ is a root of an irreducible polynomial $f(x)$ of K$[x]$, and $\alpha_1 + \alpha_2$ is a root of an irreducible polynomial $g(x)$ of K$[x]$. The roots $\beta' = \alpha_1\alpha_2$, β'', …, β^r of $f(x)$ are all different as the characteristic of K is 0, and similarly the roots $\gamma' = \alpha_1 + \alpha_2$, γ'', …, γ^s of $g(x)$ are all different. Hence from (3) the elements $\beta^i + c\,\gamma^k$ are all different. We therefore can apply the lemma of 2-72 to the field $K(\beta', \gamma')$. Thus $\beta' + c\,\gamma'$ is a primitive element of $K(\alpha_1\alpha_2, \alpha_1 + \alpha_2) = K(\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2))$; hence $\alpha_1\alpha_2$ and $\alpha_1 + \alpha_2$ belong to Λ. α_1 and α_2 are the roots of a polynomial of $\Lambda[x]$ of degree 2. Hence α_1 and α_2 are elements of Λ; $\psi(x)$ has therefore roots in Λ.

2. Let $\psi(x)$ be a polynomial of $\Lambda[x]$. To prove that $\psi(x)$ has a root in Λ, consider the automorphisms of Λ as an extension of K. As $[\Lambda : K] = 2$, any primitive element say α of Λ is a root of a quadratic polynomial which is irreducible in K$[x]$, but reduced in $\Lambda[x]$ to $a(x - \alpha)(x - \bar{\alpha})$. Hence Λ is a normal extension of K (see 3-74), and there exists an automorphism A of Λ which interchanges α and $\bar{\alpha}$, whereas the elements of K remain invariant (see 2-742). The polynomial $\psi(x)$ is transformed by A into $\bar{\psi}(x)$ and β is transformed into a conjugate element. Then $\psi(x)\,\bar{\psi}(x) = P(x)$ is a polynomial of K$[x]$ and has therefore a root, say β in Λ. Since β is a root of $P(x)$, it is a root of $\psi(x)$ or a root of $\bar{\psi}(x)$; if β is a root of $\bar{\psi}(x)$, then its conjugate is a root of $\psi(x)$. At any rate, $\psi(x)$ has a root in Λ, and as it is supposed to be irreducible, it is of degree 1; therefore every root of $\psi(x)$ belongs to Λ. Hence the theorem.

It is easy to show that the suppositions of theorem 1 are satisfied if K is taken as the field of all the real numbers, and Λ as the field of all the complex numbers. Of course, the characteristic of both the fields is equal to 0, moreover $\Lambda = K(i)$, and therefore $[\Lambda : K] = 2$. Let $f(x)$ be a polynomial of an odd degree in $K[x]$, say $f(x) = x^{2n+1} + a_1 x^{2n} + \ldots + a_{2n+1}$, put

$$c = 1 + |a_1| + \ldots + |a_{2n+1}|,$$

then there is $f(c) > 0$ and $f(-c) < 0$. Hence there exists a real number b in the interval $(-c, +c)$ for which $f(b) = 0$ holds. Thus every polynomial of an odd degree with real coefficients has a root in K. Finally, every quadratic polynomial of $\Lambda[x]$ has roots in Λ, since one can find them by extracting square roots. Hence the suppositions of theorem 1 are satisfied, and therefore the following theorem holds :

Fundamental theorem of Classical Algebra. The field of the complex numbers is closed.

Corollary. Every algebraic extension of the field K of the real numbers is isomorphic to $K(i)$.

Proof. Let Λ be an algebraic extension of K and α be an element of Λ not belonging to K. Since α is a root of a polynomial of $K[x]$, $K(\alpha)$ is isomorphic to a subfield of $K(i)$ different from K, and as $[K(i) : K] = 2$, $K(\alpha)$ is isomorphic to $K(i)$. Hence $K(\alpha)$ is closed; every element of Λ is algebraic to K, and therefore it must be an element of $K(\alpha)$. Hence $\Lambda = K(\alpha)$.

The fundamental theorem of classical algebra can be expressed also in the form : "*Every polynomial with complex coefficients* (which *e.g.* may be real and in particular may be rational) *has complex roots, and can therefore be represented as a product of linear polynomials with complex coefficients.*"

CHAPTER IV

CONTINUED FRACTIONS

4·1. *General properties of continued fractions.*

A real number $\alpha > 1$ can be approximated by an integral number s up to an error < 1, say

$$s \leqq \alpha < s + 1;$$

then

$$\alpha = s + \beta,$$

where either

$$\beta = 0,$$

or

$$1 : \beta = \alpha' > 1.$$

In the second case, α' can be approximated again by an integral number and so on. This method leads to the representation of real numbers by *continued fractions** which has many interesting properties; these will be considered in particular in 4·2 and 4·3. The underlying principle is however more general; for the integral numbers as well as for the real numbers > 1 one may substitute other systems of mathematical objects. The interconnection between the system A of the real numbers > 1 and the domain of the integral numbers which has been used in the consideration above and which will be used in the general portion of the theory is the following only:

1. The system A and the domain of the integral numbers are subsets of the same field (the field of the real numbers).

2. In this field, the domain generates a partition into classes of residues, and the elements of A are distributed among these classes in such a way that if any element α of A belongs to a particular class, then the same class contains an element $\beta = \alpha - s$ which is the inverse element of an element α' of A, unless the class of residues is the class (0), *i.e.* the class formed by the domain itself.

---

* Or *simple* continued fractions. Since in this book no other class of continued fractions is used, the notation *continued fraction* is applied here in this special sense.

Thus the investigation of the continued fractions will start here from a field K containing an integral domain S and a subsystem A which are interconnected in the manner explained just before.

4·11. *Convergents of a continued fraction.* Let K be a field, S an integral domain in K, and A be a subset of K with the following property: If a class of residues $\neq (0)$ of S contains an element of A, this class contains also the inverse of an element of A. Hence if

$$\alpha,\ \alpha',\ \alpha'',\ \ldots,\ \alpha_1,\ \alpha_2,\ \ldots \tag{1}$$

denote elements of A and

$$s,\ s',\ s'',\ \ldots,\ s_1,\ s_2,\ \ldots \tag{2}$$

denote elements of S, then every element of A can either be expressed as

$$\alpha = s + 1 : \alpha' \tag{3}$$

or as

$$\alpha = s. \tag{3'}$$

Put

$$\begin{aligned} \alpha_1 &= s_1 + 1 : \alpha_2 \\ \alpha_2 &= s_2 + 1 : \alpha_3 \\ &\cdots\cdots\cdots\cdots \\ \alpha_n &= s_n + 1 : \alpha_{n+1}, \end{aligned} \tag{4}$$

then

$$\alpha_1 = s_1 + \cfrac{1}{s_2 + \cfrac{1}{s_3 + \cfrac{\ddots}{s_n + \cfrac{\alpha_{n+1}}{1}.}}} \tag{5}$$

The representation of α_1 by (5) is said to be a *continued fraction*. The sequence of the formulas (4) can be continued indefinitely, unless there is an element α_i which is an element of S. If there is an m such that $\alpha_m = s_m$, then the continued fraction is called *finite*, otherwise it is called *infinite*. If α can be represented by a finite continued fraction, it belongs to the quotient field Q of S, and every finite set of elements

$$s_1,\ \ldots,\ s_m \tag{6}$$

of S defines an element of Q by the help of (5).

Determine now sequences of elements of S by the following formulas:

$$\begin{aligned} P_{-1} &= 0, & Q_{-1} &= 1, \\ P_0 &= 1, & Q_0 &= 0, \\ &\cdots\cdots & &\cdots\cdots \\ P_k &= s_k P_{k-1} + P_{k-2}, & Q_k &= s_k Q_{k-1} + Q_{k-2}, \end{aligned} \tag{7}$$

$$k = 1, 2, \ldots \; .$$

Let
$$D_k = \begin{vmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{vmatrix}, \tag{8}$$

then from (7) and (8) it follows that $D_k = - D_{k-1}$, and since $D_0 = 1$,

$$D_k = (-1)^k. \tag{9}$$

From (8) and (9) it follows that P_k and Q_k have no common factors in S other than unities and that

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}. \tag{10}$$

The formulas (4) can be transformed into an homogeneous form as follows:

Let a_1 be an arbitrary element $\neq 0$ of K, then a sequence of elements $a_1, a_2, \ldots, a_{n+2}$ is uniquely determined by

$$\alpha_i = a_i : a_{i+1}, \tag{11}$$

and by multiplying the equation (4) with $a_2, a_3, \ldots$ respectively, one gets

$$a_i = s_i a_{i+1} + a_{i+2}, \quad \text{for i} = 1, \ldots, \text{n}. \tag{4'}$$

From (4′) and (7) follows:

$$\begin{aligned} P_k a_{k+1} + P_{k-1} a_{k+2} &= P_{k-1} (s_k a_{k+1} + a_{k+2}) + P_{k-2} a_{k+1} \\ &= P_{k-1} a_k + P_{k-2} a_{k+1}. \end{aligned}$$

A repeated application of this formula shows that for i < k,

$$P_k a_{k+1} + P_{k-1} a_{k+2} = P_i a_{i+1} + P_{i-1} a_{i+2} = P_0 a_1 + P_{-1} a_2 = a_1.$$

Similarly (12)

$$Q_k a_{k+1} + Q_{k-1} a_{k+2} = Q_i a_{i+1} + Q_{i-1} a_{i+2} = Q_0 a_1 + Q_{-1} a_2 = a_2.$$

Hence

$$\frac{P_k \alpha_{k+1} + P_{k-1}}{Q_k \alpha_{k+1} + Q_{k-1}} = \frac{P_i \alpha_{i+1} + P_{i-1}}{Q_i \alpha_{i+1} + Q_{i-1}} = \alpha_1. \tag{13}$$

Multiply the first equation of (12) with Q_{k-1}, the second with $- P_{k-1}$ and add, then it follows from (9) that

$$(-1)^k a_{k+1} = a_1 Q_{k-1} - a_2 P_{k-1}. \tag{14}$$

From (11), (12), (13), and (9) it follows that

$$\alpha_1 - \frac{P_k}{Q_k} = \frac{(-1)^{k-1} a_{k+2}}{a_2 \quad Q_k}. \tag{15}$$

Hence if the continued fraction is finite, say $\alpha_n = s_n$, and therefore $a_{n+2} = 0$, then

$$\alpha_1 = \frac{P_n}{Q_n}. \tag{15'}$$

The elements $s_1, s_2, \ldots, s_n$ of (4) are said to be the *elements* of the continued fraction; the quotients $P_k : Q_k$ are the *convergents* and α_{n+1} is called a *complete fraction*. As α_1 is uniquely defined by these elements, we shall denote α_1, if α_{n+1} exists, by

$$\alpha_1 = (s_1, \ldots, s_n \,|\, \alpha_{n+1}) = \frac{P_n \alpha_{n+1} + P_{n-1}}{Q_n \alpha_{n+1} + Q_{n-1}},$$

and if s_n is the last element of the continued fraction, by

$$\alpha_1 = (s_1, \ldots, s_n) = \frac{P_n}{Q_n}.$$

From (4), (5′), (6′) it follows that for $k \leq n$

$$\alpha_k = (s_k, \ldots, s_n \,|\, \alpha_{n+1}),$$

or

$$\alpha_k = (s_k, \ldots, s_n), \tag{5''}$$

as the case may be. Conversely, let $\alpha_1 = (s_1, \ldots, s_{k-1} \,|\, \alpha_k)$, and α_k be given by (5″), then the expansion of α_1 into a continued fraction furnishes (5′) or (6′) corresponding to the two cases of (5″). Put k = t; as $\alpha_t, \alpha_{t+1}, \ldots$ are complete fractions obtained by expanding α_t into a continued fraction, it follows from (1) that $\alpha_t = a_t : a_{t+1}, \ldots, \alpha_{t+i} = a_{t+i} : a_{t+i+1}$.

The terms P'_i and Q'_i corresponding to α_t are determined by

$$\begin{aligned} &P'_{-1} = 0, \quad P'_0 = 1, \quad P'_i = s_{t+i-1} \; P_{i-1} + P'_{i-2} \\ &Q'_{-1} = 1, \quad Q'_0 = 0, \quad Q'_i = s_{t+i-1} \, Q'_{i-1} + Q'_{i-2}. \end{aligned} \tag{16}$$

By applying (12), (13), (14) and (9) to the expansion of α_t into a continued fraction, one gets therefore the following system of formulas:

$$\begin{aligned} \alpha_t &= P'_i \, \alpha_{t+i} + P'_{i-1} \, \alpha_{t+i+1}, \\ \alpha_{t+1} &= Q'_i \, \alpha_{t+i} + Q'_{i-1} \, \alpha_{t+i+1}, \\ (-1)^i \alpha_{t+i} &= - Q'_{i-1} \, \alpha_t + P'_{i-1} \, \alpha_{t+1}, \end{aligned} \tag{17}$$

$$\alpha_t = \frac{P'_i \; \alpha_{t+1} + P'_{i-1}}{Q'_i \; \alpha_{t+1} + Q'_{i-1}},$$

$$\begin{vmatrix} P'_i & P'_{i-1} \\ Q'_i & Q'_{i-1} \end{vmatrix} = (-1)^i.$$

4-12. *Finite continued fractions.* Without loss of generality, one may suppose that all the elements of the quotientfield $Q(S)$ of the domain S belong to the set A. As the terms P_n and Q_n of any element α_1 of A belong to S, their quotients belong to $Q(S)$. In particular, the expansion of $P_n : P_{n-1}$ and $Q_n : Q_{n-1}$ in the homogeneous form (4′) of 4-11 can be derived directly from the expansion of α_1. It is given by the formulas

$$\begin{aligned} P_n &= s_n \; P_{n-1} + P_{n-2} & \qquad Q_n &= s_n \; Q_{n-1} + Q_{n-2} \\ P_{n-1} &= s_{n-1} P_{n-2} + P_{n-3} & Q_{n-1} &= s_{n-1} Q_{n-2} + Q_{n-3} \\ &\cdots\cdots\cdots\cdots & &\cdots\cdots\cdots\cdots \\ P_1 &= s_1 & Q_2 &= s_2 \\ P_0 &= 1 & Q_1 &= 1. \end{aligned}$$

Hence

$$\frac{P_n}{P_{n-1}} = (s_n, \ldots, s_2, s_1) \qquad \frac{Q_n}{Q_{n-1}} = (s_n, \ldots, s_2). \tag{1}$$

If S is the domain of the integral numbers, it is easy to show (and it will be proved later) that an element can be expanded into a finite continued fraction if and only if it belongs to the field $Q(S)$ which — in this particular case — is the field of the rational numbers. It is interresting to study the same question under more general conditions; a close connection between continued fractions and the factorisation of S will become apparent.

Let α_1 be represented by a finite continued fraction $\alpha_1 = (s_1, \ldots, s_n)$. Then $a_n : a_{n+1} = \alpha_n = s_n$. Hence $a_n = s_n \, a_{n+1} + 0$, thus $a_{n+2} = 0$. From (12) and (14) of 4-11, one gets therefore

$$\begin{gathered} a_1 = \mathrm{P}_n \, a_{n+1}, \; a_2 = \mathrm{Q}_n \, a_{n+1} \\ (-1)^n \, a_{n+1} = a_1 \, \mathrm{Q}_{n-1} - a_2 \, \mathrm{P}_{n-1}. \end{gathered} \tag{2}$$

Hence $\alpha_1 = \mathrm{P}_n : \mathrm{Q}_n$ belongs to the quotientfield of S.

Every common factor of a_1 and a_2 is a factor of a_{n+1}, and a_{n+1} is a common factor of a_1 and a_2. Hence a_1 and a_2 have an *h. c. f.* and it can be represented linearly by a_1 and a_2. Especially $\alpha_1 = \mathrm{P}_n : \mathrm{Q}_n$ is a representation by two relatively prime-elements of S, as

$$\mathrm{P}_n \, \mathrm{Q}_{n-1} - \mathrm{Q}_n \, \mathrm{P}_{n-1} = (-1)^n.$$

Suppose every element of $Q(S)$ is representable by a finite continued fraction, and let $s', s'' \neq 0$ be two arbitrary elements of S, then $s' : s'' = \alpha$ can be represented by two relatively prime-elements of S, so that 1 can be represented in a linear and homogeneous manner by those elements.

Hence

$$s' : s'' = p : q \quad \text{and} \quad pq' + qp' = 1.$$

Therefore

$$s'q = s''p \quad \text{and} \quad s''pq' + s''qp' = s'' = q(s'q' + s''p') = qs.$$

Hence $s' = ps$, $s'q' + s''p' = s$. So the arbitrary elements s', s'' of S have an *h.c.f.* $(s', s'') = s$ which is represented in a linear and homogeneous manner by s' and s''. Thus S is a Euclidean domain (see 2-44).

If therefore S is an integral domain other than a Euclidean one, not every element of $Q(S)$ can be represented as a finite continued fraction, though all these fractions belong to $Q(S)$. The system of all the finite continued fractions is a subset of $Q(S)$ which contains S, and therefore it is not a field, unless S is a Euclidean domain.

Let a function $\mathrm{N}(s)$ which takes positive integral values only, be defined for every element $s \neq 0$ of S, and to every pair of elements s, s' of S, let there exist two other elements s_1 and s'' so that

$$s = s_1 \, s' + s'' \qquad \text{implies}$$

$$\text{either} \qquad s'' = 0, \qquad \text{or} \qquad \mathrm{N}(s'') < \mathrm{N}(s'). \tag{3}$$

Then $\quad s : s' = (s_1 | s' : s'') = (s_1, s_2 | s'' : s''') = \ldots$, and as

$$N(s') > N(s'') > N(s''') \ldots > 0$$

are all integral numbers, the sequence $s', s'', \ldots$ must be finite, hence $s : s'$ is a finite continued fraction. From these considerations the following theorem results :

Theorem. Let S be an integral domain, and let a positive integer $N(s)$ be defined satisfying the conditions (3) for every element s of S, then $Q(S)$ will be formed by the finite continued fractions of S, and the highest common factor of two elements a_1 and a_2 of S is given by a_{n+1} in (2), where P_{n-1}, Q_{n-1} have the same significance as in 4·11.

If S is the domain of the integral numbers, $N(s) = |s|$ satisfies (3) ; hence every rational number can be expanded into a finite continued fraction with integral elements, and conversely, every finite continued fraction with integral elements represents a rational number. In general, the elements of S are not supposed to be factorisable ; in particular the condition $N(ab) \geqq N(a)$, which was stated in 2·42, may not hold. If it holds in addition to (3), then S is a Euclidean domain, and therefore the factorisation in S is unique (see 2·44).

4·13. *Proper and improper equivalence.* The formulas (12), (13) and (14) of 4·11 show that the complete fractions $\alpha_1, \alpha_2, \ldots$ of a continued fraction are interconnected by linear equations. These can either be expressed in a homogeneous form

$$\begin{aligned} a_1 &= P_k\ a_{k+1} + P_{k-1}\ a_{k+2} \qquad & (-1)^k\ a_{k+1} &= Q_{k-1}\ a_1 - P_{k-1}\ a_2 \\ a_2 &= Q_k\ a_{k+1} + Q_{k-1}\ a_{k+2} \qquad & (-1)^k\ a_{k+2} &= -Q_k\ \ a_1 + P_k\ \ a_2, \end{aligned}$$

or in the non-homogeneous form as linear fractional equations

$$\alpha_1 = \frac{P_1\ \alpha_{k+1} + P_{k-1}}{Q_k\ \alpha_{k+1} + Q_{k-1}} \qquad\qquad \alpha_{k+1} = \frac{Q_{k-1}\ \alpha_1 - P_{k-1}}{-Q_k\ \ \alpha_1 + P_k}.$$

The coefficients of this substitution are elements of S, and the determinant is equal to ± 1. These substitutions will now be considered somewhat more closely. Let A and B be the matrices of such substitutions, say

$$\begin{aligned} &A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \quad \begin{matrix} \det A = \varepsilon \ = \pm 1 \\ \det B = \varepsilon' = \pm 1 \end{matrix} \\ &A' = \begin{pmatrix} \varepsilon a_4 & -\varepsilon a_2 \\ -\varepsilon a_3 & \varepsilon a_1 \end{pmatrix}, \qquad E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \end{aligned} \tag{1}$$

let α be transformed by A into α', and let α' be transformed by B into α'', then (see pp. 43—48) :

1. α is transformed by E into α, and det E $= 1$
2. α' is " " A' into α, and det A' $= \varepsilon$
3. α is " " BA into α'', and det BA $= \varepsilon\varepsilon' = \pm 1$.

An element of K is said to be *equivalent* to α if one gets it by transforming α by a linear fractional substitution with determinant ± 1. From 1, 2 and 3 it follows that this equivalence satisfies the conditions of reflexivity, symmetry and transitivity (see 2-12), and therefore this equivalence defines a partition of K into classes, so that two elements of K are equivalent if and only if they belong to the same class.

By $\begin{pmatrix} s+1 & -1 \\ 1 & 0 \end{pmatrix}$ the element 1 is transformed into s, hence all elements of S are equivalent. From 4-11, (8) and (13) it follows that complete fractions $\alpha_1, \alpha_2 \ldots$ of a continued fraction are all equivalent. So more particularly, every finite continued fraction $(s_1, \ldots, s_n)$ is equivalent to $\alpha_n = s_n$, and therefore belongs to the class containing the elements of S.

An equivalence is called *proper*, or *improper*, according as det A $= +1$, or det A $= -1$. As det A = det A', the notion of proper equivalence as well as the notion of improper equivalence is a symmetric one. By combining two equivalences of the same kind, one gets a proper equivalence, and by combining two equivalences of different kinds, an improper equivalence. Every element is properly equivalent to itself, for the matrix E has the determinant 1. If in a class of equivalent elements, an element is also improperly equivalent to itself, *i.e.* if α is transformed into α by E', and det E' $= -1$, then an arbitrary element β of the same class is transformed into α by B and by E'B. One of these matrices has the determinant 1, the other has the determinant -1, so each element of the class is properly and improperly equivalent to α, and therefore every element is at the same time properly and improperly equivalent to every other element of the class. If on the other hand α is transformed into β by A as well as by B, where det A $= 1$, det B $= -1$, then α is transformed into α by A'B, where det A'B $= -1$, and therefore α is improperly equivalent to itself, so that in this case, every other element of the class (α) is properly and improperly equivalent to every other element of (α). If in (α) there are no pairs of elements properly as well as improperly equivalent, then (α) must be divided into two classes without common elements ; the elements of the first class are properly, and the elements of the second class are improperly equivalent to α. Elements of the same sub-class are properly equivalent, elements of different sub-classes are improperly equivalent. Hence :

Theorem. In a class of equivalent elements, either every element is properly and improperly equivalent to every other element, or there are two sub-classes without common element, such that elements of the same sub-class are properly, and of different sub-classes are improperly equivalent.

As I is transformed into itself by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, every pair of elements is properly and improperly equivalent in the class containing the finite continued fractions.

Let α be transformed into itself by A. Then

$$\alpha = \frac{a_1\,\alpha + a_2}{a_3\,\alpha + a_4} \text{ holds, hence } a_3\alpha^2 + (a_4 - a_1)\,\alpha - a_2 = 0. \qquad (2)$$

There are 3 different cases :

1. $a_3 = (a_4 - a_1) = a_2 = 0$. In this case A = E or − E.

By these transformations every element is transformed into itself. E and − E generate proper equivalences.

2. The polynomial (2) is reducible in α. This is possible only if α is an element of the quotientfield Q of S.

3. The polynomial (2) is irreducible. In this case α is algebraic to Q and of order 2 over Q.

From these considerations it follows that there are elements which are not improperly equivalent to themselves.

Let the complete fractions $\alpha_1, \alpha_2, \ldots$ of the continued fraction not be all different, say

$$\alpha_i = \alpha_{i+l}, \text{ then}$$

$$\alpha_i = (s_i, \ldots, s_{i+l-1} | \alpha_i) = (s_{i+1}, \ldots, s_{i+l}, s_{i+1}, \ldots, s_{i+l} | \alpha_i).$$

Hence α_i can be represented by an infinite periodic continued fraction with the period $s_{i+1}, \ldots, s_{i+l}$. From 4-11, (17) it follows that α_i is transformed into itself by the matrix $D = \begin{pmatrix} P'_l & P'_{l-1} \\ Q'_l & Q'_{l-1} \end{pmatrix}$, where $\det D = (-1)^l$, and therefore α_i is made equivalent to itself by that transformation. From

4-11, (13) it follows that $\alpha_i = \dfrac{P_{i-1}\,\alpha_i + P_{i-2}}{Q_{i-1}\,\alpha_i = Q_{i-2}}$ and therefore it belongs to the field $Q(\alpha_i)$. Hence $[Q(\alpha_1) : Q] \leqq 2$, thus α_1 satisfies an equation of degree 2 with coefficients from Q, and as Q is the quotient field of S, one can arrange by multiplication with a suitable common factor that the coefficients belong to S. The same holds for $\alpha_2, \alpha_3 \ldots$

Let now a periodic sequence $a_1, \ldots, a_m, a_1, \ldots, a_m, \ldots$ of elements of S be given. Then one does not know whether in any extension of the quotientfield Q of S there exists an element representable by the infinite periodic continued fraction

$$(a_1, \ldots, a_m, a_1, \ldots, a_m, \ldots), \tag{3}$$

and if such an element exists, it may not be uniquely determined in the field. But if there is a field in which there exists one and only one element α represented by the periodic continued fraction (3), then

$$\alpha = (a_1, \ldots, a_m, a_1, \ldots, a_m, \ldots) = (a_1, \ldots, a_m \,|\, \alpha)$$

holds and therefore α is a root of a quadratic polynomial in $S[x]$. The same holds for $\beta = (b_1, \ldots, b_t \,|\, \alpha) = (b_1, \ldots, b_t, a_1, \ldots, a_m, a_1, \ldots)$ as this number can be transformed into α by a linear transformation in Q.

4·2. *Representation of the positive numbers by continued fractions.*

4·21. *Correspondence between positive numbers and rational positive expansions.* Let the elements of the set A be the real numbers $\geqq 1$, and let S be the ring of the integers ; then the representation

$$\alpha = s + 1 : \alpha' \qquad \text{or } \alpha = s$$

is always possible. If α is not an integral number, then

$$1 < s < \alpha < s + 1, \quad \alpha' = 1 : (\alpha - s),$$

and this representation is unique. But if α is an integral positive number,

$\alpha = s' + 1,\ s' = 0, 1, 2, \ldots$, there exist two possibilities

$$\begin{aligned} &1.\quad s = s',\ \alpha' = 1 \\ &2.\quad s = s' + 1. \end{aligned} \tag{1}$$

Therefore in the representation 4-11, (4) of any positive α as a continued fraction,

$$\begin{aligned} &s_1 \qquad \text{is a non-negative integral number, and} \\ &s_2, s_3, \ldots \text{ are positive integral numbers.} \end{aligned} \tag{2}$$

As has been shown in 4-12, the rational numbers can be represented by finite continued fractions.

Let α_1 be a rational number $\geqq 1$. If α_1 is an integral number, then there are the two representations of α_1 corresponding to the two cases in (1)

$$\alpha_1 = (s' + 1)$$

and

$$\alpha_1 = s' + \tfrac{1}{1}.$$

If α_1 is not integral, α_2 is uniquely determined by α_1; if α_2 is not integral, α_3 is uniquely determined by α_2, etc. There is no possibility for alteration in the sequence $\alpha_1, \alpha_2, \ldots$ so long as these elements are not integral; α_1 admits a representation by a finite continued fraction, the last complete fraction in it is necessarily integral. Let α_{r+1} $(r > 0)$ be the first integral complete fraction which occurs; then $\alpha_r = s_r + 1 : \alpha_{r+1}$ is not integral, $1 < \alpha_{r+1} = s' + 1$, where $s' > 0$. Thus there are two possibilities for the continuation of the continued fraction:

$$s_{r+1} = (s' + 1), \text{ or } s_{r+1} = s', \ \alpha_{r+1} = 1,$$

and there exist two and only two representations of α_1

$$\alpha_1 = (s_1, \ldots, s_r, s' + 1), \text{ and } \alpha_1 = (s_1, \ldots, s_r, s', 1).$$

If $\alpha_1 > 1$ is irrational, then $s_1 > 0$, and $\alpha_2, \alpha_3 \ldots$ are uniquely determined, none of them being rational; hence there exists one and only one representation satisfying (2), and this continued fraction is infinite. If $0 < \beta < 1$, then $\dfrac{1}{\beta} = \alpha > 1$, and $\beta = (0 \mid \alpha)$. The essence of these considerations is given by the following theorem:

Theorem 1. Every positive number can be represented as a continued fraction satisfying the conditions (2). If the number is irrational, the representation is unique and the continued fraction is infinite. If the number is rational, there exist two representations, one by an even finite continued fraction and the other by an odd finite continued fraction.

It will be proved now that the converse theorem also holds, *i.e.* every sequence satisfying (2) determines one and only one real number.

Let $s_1, s_2, \ldots$ be an infinite sequence satisfying the conditions (2). Put

$$\mathrm{P}_{-1} = 0,\ \mathrm{P}_0 = 1,\ \mathrm{P}_1 = s_1,\ \mathrm{P}_2 = s_2\,\mathrm{P}_1 + 1,\ \mathrm{P}_k = s_k\,\mathrm{P}_{k-1} + \mathrm{P}_{k-2},$$
$$\mathrm{Q}_{-1} = 1,\ \mathrm{Q}_0 = 0,\ \mathrm{Q}_1 = 1,\ \mathrm{Q}_2 = s_2,\qquad \mathrm{Q}_k = s_k\,\mathrm{Q}_{k-1} + \mathrm{Q}_{k-2}.$$

From $P_2 > 0, Q_1 > 0$, it follows by mathematical induction that

$$\begin{aligned} &Q_2, Q_3, \ldots, P_0, P_2, \ldots > 0 \text{ and that} \\ &0 \leqq P_1 < P_2 < P_3 \ldots < \ldots \\ &Q_0 = 0 < Q_1 \leqq Q_2 < Q_3, \ldots < \ldots \text{ hold.} \end{aligned} \tag{3}$$

These inequalities hold independently, whether there exists a number $\alpha_1 = (s_1, s_2, \ldots,)$, or not. Suppose in particular that α_1 exists, then $P_k : Q_k$ are its convergents (for $k = 1, 2, \ldots$) ; applying the homogeneous notations $\alpha_i = a_i : a_{i+1}$ as in 4-11, one may select $a_1 > 0$; then every a_i is greater then zero. Therefore (see 4-11, (15)) :

$$\alpha_1 = \frac{P_k}{Q_k} - \frac{(-1)^{k+1} \; a_{k+2}}{a_2 \quad Q_2} \begin{matrix} > 0 \text{ if } k \geqq 1 \text{ is odd} \\ < 0 \;\; ,, \; k > 1 \text{ is even.} \end{matrix} \tag{4}$$

Hence :

$$\frac{P_{2m}}{Q_{2m}} > \alpha_1 > \frac{P_{2m-1}}{Q_{2m-1}}, \text{ for } m = 1, 2, \ldots \tag{5}$$

Now, the finite continued fractions $(s_1, s_2, \ldots, s_n) = P_n : Q_n$ exist at any rate (even if $(s_1, s_2, \ldots)$ does not exist), and $(s_1, \ldots, s_k)$ is its k^{th} convergent, provided $k < n$. By applying (5) to $\alpha_1 = \frac{P_n}{Q_n}$ one obtains for $n > 2m$

$$\frac{P_{2m}}{Q_{2m}} > \frac{P_n}{Q_n} > \frac{P_{2m-1}}{Q_{2m-1}}. \quad \text{Hence}$$

$$\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \ldots < \frac{P_{2m+1}}{Q_{2m+1}}, \quad \frac{P_2}{Q_2} > \frac{P_4}{Q_4} > \ldots > \frac{P_{2m}}{Q_{2m}}, \tag{6}$$

for $m = 1, 2, 3, \ldots$

Thus the quotients $\frac{P_n}{Q_n}$ form two sequences, one is increasing, the other decreasing, and every number of the first sequence is less than every number of the second one. The intervals $\left(\frac{P_{2n-1}}{Q_{2n-1}}, \frac{P_{2n}}{Q_{2n}}\right)$ form therefore a nest of intervals,

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_k \; Q_{k-1}} \qquad \text{(see 4-11, (10)).}$$

The length of these intervals converges to 0. Hence there is, for every given sequence (2), one and only one real number α, so that

$$\frac{P_{2m}}{Q_{2m}} > \alpha > \frac{P_{2m-1}}{Q_{2m-1}} \quad \text{holds for } m = 1, 2, \ldots \tag{7}$$

If there exists a number $\alpha_1 = (s_1, s_2, \ldots)$, then α_1 must satisfy the inequalities (5); thus by comparison of (5) and (7), it follows from the uniqueness of the solution of (7) that $\alpha = \alpha_1$, provided that there exists a number which can be expanded into the infinite continued fraction $(s_1, s_2, \ldots)$. To prove the existence of this number, the following lemma is helpful.

Lemma. Let t be a positive integral number, $(s_1, \ldots, s_n, s_{n+1}) = \mathrm{A}$, $(s_1, \ldots, s_n + t) = \mathrm{B}$, then

$$\begin{aligned} \mathrm{A} - \mathrm{B} &\geqq 0 \qquad \text{if } n \text{ is even,} \\ &\leqq 0 \qquad \text{if } n \text{ is odd,} \end{aligned} \tag{8}$$

equality holds in (8) if and only if $t = s_{n+1} = 1$.

Proof. Apply the usual notations, and put

$$\mathrm{Q}' = (s_n + t)\mathrm{Q}_{n-1} + \mathrm{Q}_{n-2} = \mathrm{Q}_n + t\ \mathrm{Q}_{n-1},$$

then

$$(\mathrm{Q}' - \mathrm{Q}_n) : \mathrm{Q}_{n-1} = t, \quad \text{and} \quad (t\mathrm{Q}_{n+1} - \mathrm{Q}') : \mathrm{Q}_n = ts_{n+1} - 1.$$

From 4·11, (10) it follows that $\mathrm{B} - \mathrm{P}_{n-1} : \mathrm{Q}_{n-1} = (-1)^n : (\mathrm{Q}_{n-1}\,\mathrm{Q}')$. Hence

$$\begin{aligned} \mathrm{A} - \mathrm{B} &= (\mathrm{A} - \mathrm{P}_n : \mathrm{Q}_n) + (\mathrm{P}_n : \mathrm{Q}_n - \mathrm{P}_{n-1} : \mathrm{Q}_{n-1}) - (\mathrm{B} - \mathrm{P}_{n-1} : \mathrm{Q}_{n-1}) \\ &= (-1)^n \left(\frac{-1}{\mathrm{Q}_n\ \mathrm{Q}_{n+1}} + \frac{1}{\mathrm{Q}_n\ \mathrm{Q}_{n-1}} - \frac{1}{\mathrm{Q}'\ \mathrm{Q}_{n-1}} \right) \\ &= (-1)^n \left(\frac{-1}{\mathrm{Q}_n\ \mathrm{Q}_{n+1}} + \frac{t}{\mathrm{Q}_n\ \mathrm{Q}'} \right) = (-1)^n \frac{ts_{n+1} - 1}{\mathrm{Q}_{n+1}\ \ \mathrm{Q}'}\,. \end{aligned} \tag{9}$$

Hence the lemma.

In a similar manner, one computes the difference $(s_1, \ldots, s_n - t) - (s_1, \ldots, s_n)$. Denote the last convergent of the first term by $\mathrm{P}'' : \mathrm{Q}''$, and the other convergents as usual, then $(\mathrm{Q}_n - \mathrm{Q}'') : \mathrm{Q}_{n-1} = t$ holds, and therefore

$$(s_1, \ldots, s_n - t) - (s_1, \ldots, s_n) = \frac{(-1)^n}{\mathrm{Q}_{n-1}} \left(\frac{1}{\mathrm{Q}''} - \frac{1}{\mathrm{Q}_n} \right) = \frac{t}{\mathrm{Q}_n\ \mathrm{Q}''}\,.$$

Hence :

$$(s_1, \ldots, s_n - t) > (s_1, \ldots, s_n) > (s_1, \ldots, s_n, \ldots, s_m), \tag{10}$$

when n is *even* and $t > 0$, whereas for an *odd* n and $t > 0$, the *converse* inequalities hold. Again, let $\mathrm{P}_i : \mathrm{Q}_i$ be the convergents of an infinite continued fraction $(s_1, s_2, \ldots)$ satisfying (2), and let α_1 be the real number which is uniquely determined by (7). This number admits an expansion into a continued fraction which will be proved to be $(s_1, s_2, \ldots)$. If not, suppose α_1 is expanded into a different continued fraction, and let it be an infinite one. Then the expansion can be expressed by $(s_1, \ldots, s_{n-1}, \sigma, \ldots)$, where $n > 0$, $\sigma \neq s_n$. Suppose $\sigma - s_n = t > 0$. If n is *even* it follows from (5), (7) and (8) that

$$\alpha_1 > (s_1, \ldots, s_n + t) \geqq (s_1, \ldots, s_{n+1}) > \alpha_1, \tag{11}$$

whereas the converse inequalities hold when n is odd. Hence $\sigma > s_n$ is impossible. If $\sigma < s_n$, put $s_n - \sigma = t$, and by interchanging the two expansions, one shows in the same way as above that the supposition leads to a contradiction. Suppose now that the expansion of α_1 is finite; then it follows from (7) that this finite continued fraction cannot be a convergent of $(s_1, s_2, \ldots)$. Hence it can be expressed by $(s_1, \ldots, s_{n-1}, \sigma, \ldots, \tau)$, where $\sigma \neq s_n$. For $\sigma > s_n$, the same argument holds as in the case of an infinite continued fraction. Similarly for $\sigma < s_n$, provided the finite continued fraction has more than n elements. It remains to show that $(s_1, \ldots, s_n - t) \neq \alpha_1$, but this follows from (10) and (7), as for an even n

$$(s_1, \ldots, s_n - t) > (s_1, \ldots, s_n) > \alpha_n,$$

whereas for an odd n, the converse inequality holds. Hence α_1 cannot be expanded into any continued fraction which is different from $(s_1, s_2, \ldots)$, therefore it is an irrational number; as every positive number can be expanded into a continued fraction, the expansion of α_1 must be $(s_1, s_2, \ldots)$. Thus the following theorem holds:

Theorem 2. Let $s_1, s_2, \ldots$ be an infinite sequence satisfying (2), then there exists a uniquely determined number $\alpha_1 = (s_1, s_2, \ldots)$. This number is irrational, and it does not admit any different expansion into a continued fraction with elements satisfying (2).

4·22. *Distribution of the continued fraction along the real axis.* By the two theorems of 4·21, it has been shown that to every continued fraction satisfying (2), there corresponds a non-negative real number; rational positive numbers can be expanded into exactly two different continued fractions which are both finite; irrational positive numbers admit one and only one expansion which is infinite, and 0 is expanded into the continued fraction with the only element $s_1 = 0$. It is interesting to investigate the distribution of the continued fractions along the real axis. The continued fractions with one element, $s_1 = 0, 1, 2, \ldots$ represent these integral numbers and subdivide the positive half of the real axis into intervals of equal length 1. The continued fractions with two elements are distributed among these intervals as follows. As $(s_1, m) = s_1 + \frac{1}{m}$, for every positive integral value of m, (s_1, m) is situated in the interval which is bounded by s_1 and $s_1 + 1$, and will be denoted by I_{s_1}. For $m = 1$, the number (s_1, m) is the right end point of the interval, and with m tending to infinity, it converges steadily to the left end. Thus every interval I_{s_1} is subdivided into an infinity of abutting subintervals $I_{s_1 s_2}$ bounded by $(s_1, s_2 + 1)$ and (s_1, s_2) which cover I_{s_1}, except its left endpoint. As $(s_1, s_2, m) = s_1 + \left(s_2 + \frac{1}{m}\right)$, each of these continued fractions lies in $I_{s_1 s_2}$ and they converge steadily from the left end of $I_{s_1 s_2}$ to its right end and intersect it into an infinity of abutting intervals $I_{s_1 s_2 s_3}$. Consider now the interval $I_{s_1 \ldots s_n}$ which is bounded by $(s_1, \ldots, s_n)$ and $(s_1, \ldots, s_n + 1)$. By applying the methods and formulas of 4-21, one finds easily :

$$\frac{(s_1, \ldots, s_n, t) - (s_1, \ldots, s_n)}{(s_1, \ldots, s_n + 1) - (s_1, \ldots, s_n)} = \frac{Q_n + Q_{n-1}}{tQ_n + Q_{n-1}}. \qquad (1)$$

The right hand side of (1) is a positive number which is equal to 1 if $t = 1$, and converges steadily to zero, when t steadily increases. Hence the points $(s_1, \ldots, s_n, t)$ converge steadily from $(s_1, \ldots, s_n + 1)$ to $(s_1, \ldots, s_n)$ when t increases ; they subdivide the interval $I_{s_1 \ldots s_n}$ into an infinity of abutting intervals, and these intervals cover $I_{s_1 \ldots s_n}$ with the only exception of $(s_1, \ldots, s_n)$. This point is the left or the right end point of $I_{s_1 \ldots s_n}$ according as n is odd or even. To every infinite sequence $s_1, s_2, \ldots$ satisfying 4-21, (2) there corresponds a sequence of intervals $I_{s_1}, I_{s_1 s_2}, \ldots$ which form a *nest*; the convergents of $(s_1, s_2, \ldots)$ are alternatively the left and the right endpoints of these intervals ; hence the nest converges to $(s_1, s_2, \ldots)$. Thus there is a (1, 1)-correspondence between the positive irrational numbers and the nests. The endpoints of the nest-intervals are rational numbers, and one gets a classification of the non-negative rational numbers in the following way. The first class contains the numbers which can be expanded into continued fractions with only one element (these numbers are integral), the numbers of the second class can be expanded into continued fractions with two (but not with one) elements etc., the m^{th} class is composed of the numbers which can be expanded into continued fractions with m (but not with $m - 1$) elements.

The importance of this classification is made evident by the following theorem.

Theorem. If $s > 0$, and $\frac{P_{2n-1}}{Q_{2n-1}} < \frac{r}{s} < \frac{P_{2n}}{Q_{2n}}$, then $s > Q_{2n} > Q_{2n-1}$.

Proof. From the supposition, it follows directly that $0 < \frac{r}{s} - \frac{P_{2n-1}}{Q_{2n-1}} < \frac{P_{2n}}{Q_{2n}} - \frac{P_{2n-1}}{Q_{2n-1}} = \frac{1}{Q_{2n}\ Q_{2n-1}}$ and as s and Q_{2n-1} are positive, $0 < r\ Q_{2n-1} - s\ P_{2n-1} < \frac{s}{Q_{2n}}$, the middle part of this inequality is an integral positive number. Hence

$$1 < \frac{s}{Q_{2n}}\ i.\ e.\ \ Q_{2n} < s.$$

This theorem shows that the closest approximations of a real number by the help of rational numbers with limited positive denominators are the approximations by the convergents $P_m : Q_m$.

Since α lies in the interval bounded by two consecutive convergents $P_n : Q_n$ and $P_{n+1} : Q_{n+1}$, its distance from $P_n : Q_n$ is less than the length of the interval. Therefore :

$$\left| \alpha - \frac{P_n}{Q_n} \right| < \left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n\ Q_{n+1}} < \frac{1}{Q_n^2}\ ; \tag{2}$$

hence

$$\alpha = \frac{P_n}{Q_n} + \frac{\varepsilon}{Q_n^2}, \tag{3}$$

where $|\varepsilon| < Q_n : Q_{n+1} < 1$, and ε is positive or negative according as n is odd or even. Thus

$$P_n = Q_n\ \alpha - \frac{\varepsilon}{Q_n}. \tag{4}$$

4·3. *Periodic continued fractions with integral coefficients.* The elements of the continued fractions considered in this article and its subsections are supposed to be integral numbers. The first element is positive or zero, the other elements are positive. A periodic continued fraction with a period $a_1, \ldots, a_m$, say

$$(b_1, \ldots, b_l,\ a_1, \ldots, a_m,\ a_1, \ldots, a_m, \ldots)$$

will be denoted by

$$(b_1, \ldots, b_l,\ \overline{a_1, \ldots, a_m}). \tag{1}$$

In the special case where there are no elements b_j, the continued fraction is said to be *purely periodic*. At any rate, (1) determines uniquely an irrational number ; thus it follows from the last paragraph of 4·13, that this number is a root of a quadratic polynomial say $f(x)$ of $R[x]$, where R denotes the field of the rational numbers. For the irrationality of the roots, $f(x)$ is irreducible in $R[x]$.

4·31. *Expansion of quadratic elements into periodic continued fractions.* The converse of the last statement is given by the following theorem.

Theorem. Let $[\Lambda : R] = 2$, then every irrational number α belonging to Λ can be expanded into a periodic continued fraction.

Proof. Let α be the root of an irreducible polynomial

$$f(x) = a\,x^2 + 2\,b\,x + c. \tag{1}$$

Expand α into a continued fraction, $\alpha = (s_1, \ldots, s_n, \lambda)$; then (see 4·11,(5′)).

$$\alpha = \frac{\mathrm{P}_n\,\lambda + \mathrm{P}_{n-1}}{\mathrm{Q}_n\,\lambda + \mathrm{Q}_{n-1}},$$

hence $a(\mathrm{P}_n\,\lambda + \mathrm{P}_{n-1})^2 + 2b(\mathrm{P}_n\,\lambda + \mathrm{P}_{n-1})\,(\mathrm{Q}_n\,\lambda + \mathrm{Q}_{n-1}) + c(\mathrm{Q}_n\,\lambda + \mathrm{Q}_{n-1})^2 = 0$; thus λ is a root of

$$gx^2 + 2h\,x + k = 0, \tag{2}$$

where

$$\begin{vmatrix} g & h \\ h & k \end{vmatrix} = \begin{vmatrix} \mathrm{P}_n & \mathrm{P}_{n-1} \\ \mathrm{Q}_n & \mathrm{Q}_{n-1} \end{vmatrix}^2 \begin{vmatrix} a & b \\ b & c \end{vmatrix} = \begin{vmatrix} a & b \\ b & c \end{vmatrix}. \tag{3}$$

Let β be the second root of (1) and μ be defined by

$$\mu = \frac{-\,\mathrm{Q}_{n-1}\,\beta + \mathrm{P}_{n-1}}{\mathrm{Q}_n\quad\beta - \mathrm{P}_n}, \qquad \text{hence} \tag{4}$$

$$\beta = \frac{\mathrm{P}_n\,\mu + \mathrm{P}_{n-1}}{\mathrm{Q}_n\,\mu + \mathrm{Q}_{n-1}}.$$

As $a\beta^2 + 2b\beta + c = 0$, the number μ satisfies (2). From (4) it follows that

$$\mu = \frac{-\,\mathrm{Q}_{n-1}}{\mathrm{Q}_n} \pm \frac{1}{\mathrm{Q}_n(\mathrm{Q}_n\,\beta - \mathrm{P}_n)}, \tag{5}$$

where $\pm$ has to be chosen according as n is odd or even.

From (5) and 4·22, (4) it follows therefore that

$$\begin{aligned} \mu &= \frac{-\,\mathrm{Q}_{n-1}}{\mathrm{Q}_n} \pm \frac{1}{\mathrm{Q}_n^2(\beta - \alpha) + \varepsilon} \\ &= \frac{-\mathrm{Q}_{n-1}}{\mathrm{Q}_n}\left(1 \pm \frac{1}{\mathrm{Q}_n\,\mathrm{Q}_{n-1}(\beta - \alpha) + \varepsilon'}\right) \\ &< 0 \text{ if } \mathrm{Q}_n\,\mathrm{Q}_{n-1}\,|\beta - \alpha| > 2. \end{aligned}$$

As Q_n increases infinitely with n, and $\beta \neq \alpha$, the root μ is negative for sufficiently high values of n, and as λ is a complete fraction and therefore positive, $\lambda\,\mu = k : g < 0$. Hence $k\,g < 0$ for all sufficiently high values of n. To each of these values, there corresponds a partition of the positive number $b^2 - ac = h^2 - kg$ (see (3)) into two non-negative summands h^2 and $-kg$; to the first term there correspond atmost 2 values $\pm h$, and to the second, a finite number of integral factors k and g. Hence (3) admits only a finite number of solutions g,h,k for which $kg < 0$ holds. Let now n run over 1, 2, ... and consider the corresponding polynomials (2); for each of these polynomials $h^2 - gk = b^2 - ac$ as (3) holds, and for sufficiently high values of n, the inequality $kg < 0$ holds. Hence the polynomials $gx^2 + 2hx + k$ cannot all be different. At least one polynomial with $kg < 0$ must occur more than once. This polynomial has exactly one positive root, which is equal to the corresponding complete fraction. Hence the complete fractions are not all different, say

$$\alpha_q = \alpha_{q+m}.$$

Hence
$$\alpha_q = (c_1, \ldots, c_m \,|\, \alpha_q) = (\overline{c_1, \ldots, c_m})$$

is represented by a purely periodic continued fraction. Hence α is represented by a periodic continued fraction.

4·32. *Purely periodic continued fractions.* Let $\alpha_1, \alpha_2, \ldots$ be the complete fractions of $(s_1, \ldots, s_m, \overline{s_{m+1}, \ldots, s_{m+k}})$. As $\alpha_i = \alpha_{i+k}$, for $i > m$, every property which holds for the complete fractions of sufficiently high index, holds for every complete fraction of index $> m$. From 4·31 one knows that the root conjugate to a complete fraction of sufficiently high index is negative. Therefore this property holds for every complete fraction of index $> m$, *i.e.*, for every purely periodic continued fraction. In a purely periodic continued fraction $s_1 = s_{k+1} \neq 0$ (see 4·2, (2)); hence these continued fractions represent numbers > 1.

A root λ of a quadratic equation is said to be *reduced* if $\lambda > 1$, and the conjugate root satisfies $0 > \mu > -1$. It will be proved now that every purely periodic continued fraction represents a reduced quadratic number.

Let

$$\alpha = (\overline{s_1, \ldots, s_n}) = (s_1, \ldots, s_n \,|\, \alpha) \tag{1}$$

$$\xi = (\overline{s_n, \ldots, s_1}) = (s_n, \ldots, s_1 \,|\, \xi) \tag{2}$$

be two purely continued fractions, the elements s_i being the same in both the continued fractions, but ordered in an inverse manner.

Let $P_j : Q_j$ be the convergents of α. Then (see 4·12, (1))

$$\frac{P_n}{P_{n-1}} = (s_n, \ldots, s_1) \text{ and } \frac{Q_n}{Q_{n-1}} = (s_n, \ldots, s_2)$$

are convergents of ξ; hence $\xi = \dfrac{P_n\ \xi + Q_n}{P_{n-1}\ \xi + Q_{n-1}}$ holds. Let $\beta = \dfrac{-1}{\xi}$, then $0 > \beta > -1$, and $P_{n-1}\ \beta^{-2} + (P_n - Q_{n-1})\ \beta^{-1} - Q_n = 0$; hence β is a root of $f(x) = Q_n\ x^2 + (Q_{n-1} - P_n)\ x - P_{n-1}$.

As $\alpha = \dfrac{P_n\ \alpha + P_{n-1}}{Q_n\ \alpha + Q_{n-1}}$, α is also a root of $f(x)$, and as $\alpha > 1$, the roots α and β are different. The essence of these considerations is therefore:

Theorem. If α is represented by a purely periodic continued fraction (1) it is a reduced quadratic number; let β be the number conjugate to α, and $\xi = -\beta^{-1}$, then ξ is represented by (2).

Every continued fraction is equivalent to its complete fractions (see 4·13); especially every periodic continued fraction is equivalent to a purely periodic continued fraction; hence

Corollary. Every quadratic number is equivalent to a reduced quadratic number.

4·33. *Scheme for calculation.* In order to find out the representation of any quadratic number α by a continued fraction, represent α by

$$\alpha = \frac{a + \sqrt{D}}{b} = s + \frac{1}{\alpha'}, \text{ where } s < \alpha < s + 1$$

and $a, b, s, D > 0$ are integral numbers.

Then

$$\alpha' = \frac{a' + \sqrt{D}}{b'},$$

where $\qquad a' = b\,s - a, \quad b' = (D - a'^2) : b.$

Starting from these formulas, a simple numerical scheme given below furnishes the numbers $a, b; a', b' \ldots$ defining uniquely the complete fractions $\alpha, \alpha', \ldots$ and the numbers $s, s', \ldots$ defining the continued fraction. As this continued fraction is periodic, one pair a, b must be repeated after a finite number of steps. Then the first period is finished and the calculation can be terminated.

Examples.

1. $\alpha = \dfrac{-1+\sqrt{5}}{2}$ (harmonic section), $D = 5$

a	b		s
-1	2	$0 < \dfrac{-1+\sqrt{5}}{2} < 1$	0
1	2	$1 < \dfrac{1+\sqrt{5}}{2} < 2$	1
1	2		

The last complete fraction is therefore equal to the preceding; hence $\alpha = (0, \overline{1})$. This continued fraction is the simplest, but the least convenient one for practical calculation, as the numbers P_k, Q_k are increasing more slowly than in any other case.

2. $\alpha = \sqrt{26}$.

a	b	s
0	1	5
5	1	10
5	1	

hence $\alpha = (5, \overline{10})$. This example is very convenient for quick and exact calculation.

$P_0 = 1$	$Q_0 = 0$
$P_1 = 5$	$Q_1 = 1$
$P_2 = 51$	$Q_2 = 10$
$P_3 = 515$	$Q_3 = 101$
$P_4 = 5201$	$Q_4 = 1020$
$P_5 = 52525$	$Q_5 = 10301$
$P_6 = 530451$	$Q_6 = 104030$

Hence $\alpha = \frac{530451}{104030} - \varepsilon$, where $0 < \varepsilon < 10^{-1}$. Therfore $\alpha = 5{\cdot}099019513(60)$, the last two figures being uncertain, (see 4-22, (3)).

3. $\alpha = \sqrt{2}$. $D = 2$

a	b	s
0	1	1
1	1	2
1	1	

Hence $\sqrt{2} = (1, \overline{2})$. As P_k, Q_k are increasing very slowly, the method will be applied in a modified form.

$$\sqrt{2} = \sqrt{200} : 10. \quad \text{If } \sqrt{200} = \frac{P_n}{Q_n} \pm \varepsilon,\ \sqrt{2} = \frac{P_n}{10Q_n} \pm \frac{\varepsilon}{10}.$$

Thus expand $\sqrt{200}$ into a continued fraction. $D = 200 = 14^2 + 4$.

a	b		s
0	1	$14 < \sqrt{200} < 15$	14
14	4	$7 < \frac{14 + \sqrt{200}}{4} < 8$	7
14	1	$28 < 14 + \sqrt{200} < 29$	28
14	4		

Hence $\sqrt{200} = (14, \overline{7, 28})$.

$P_0 = 1$ $\qquad Q_0 = 0$

$P_1 = 14$ $\qquad Q_1 = 1$

$P_2 = 99$ $\qquad Q_2 = 7$

$P_3 = 2786$ $\qquad Q_3 = 197$

$P_4 = 19601$ $\qquad Q_4 = 1386$

$$\sqrt{200} = \frac{19601}{1386} - \varepsilon,\ 0 < \varepsilon < \frac{1}{Q_4\, Q_5} < \frac{1}{28\, Q_4^2} < 3{\cdot}10^{-8}$$

$$\sqrt{2} = \frac{19601}{13860} - \varepsilon',\ = 1.41421356\ (4),$$

correct up to eight figures after the decimal point, as $0 < \varepsilon' < 3{\cdot}10^{-9}$.

Exercises. Prove that $(a, \overline{2a}) = \sqrt{(a^2 + 1)}$, and calculate $\sqrt{2501}$, $\sqrt{82}$, $\frac{\sqrt{7} + 2}{3}$, $\sqrt{17}$. Calculate $\sqrt{3}$ directly and also by the help of $\sqrt{300}$. Compute $\sqrt{(a^2 + \frac{1}{2})}$.

4·34. *Reduced quadratic numbers.* To prove the converse proposition of the theorem of 4·32, the following lemma is useful.

Lemma. If $\alpha > 1$ and $\beta < 0$ are conjugate quadratic numbers, $\alpha = (s, s_1, s_2, \ldots)$, then all the complete fractions $\alpha_1 = (s_1, s_2, \ldots)$, $\alpha_2 = (s_2, \ldots)$ are reduced numbers.

Proof. $\alpha = s + \frac{1}{\alpha_1}$, $\beta = s + \frac{1}{\beta_1}$, α_1 and β_1 are conjugate numbers $\alpha_1 > 1$, $\frac{-1}{\beta_1} = s - \beta > s \geqq 1$; hence α_1 is reduced, and by repetition of this procedure it follows that $\alpha_2, \ldots$ are reduced.

Theorem. Every reduced quadratic number is represented by a purely periodic continued fraction.

Proof. Every quadratic number is represented by a periodic continued fraction $(a, \ldots, s, \overline{s_1, \ldots, s_n})$. Let this number be reduced and let the periodicity of the continued fraction begin with s_1 only (*i.e.* let $s \neq s_n$), then it follows from the last lemma that $(s, \overline{s_1, \ldots, s_n})$ is a reduced number too. We will prove that this is impossible. Using the same notations as in the lemma we state

$$\alpha_1 = \alpha_{n+1}, \qquad \text{hence } \beta_1 = \beta_{n+1}$$

$$\alpha = s + \frac{1}{\alpha_1}, \alpha_n = s_n + \frac{1}{\alpha_{n+1}}, \text{ hence } \beta = s + \frac{1}{\beta_1}, \beta_n = s + \frac{1}{\beta_{n+1}}$$

$$\frac{-1}{\beta_1} = s - \beta, \frac{-1}{\beta_{n+1}} = s_n - \beta_n;$$

but as α and α_n are reduced, $0 < -\beta < 1$, and $0 < -\beta_n < 1$ hold; hence $s < \frac{-1}{\beta_1} < s + 1$, and $s_n < \frac{-1}{\beta_{n+1}} < s_{n,n} + 1$. From $\beta_1 = \beta_{n+1}$ it follows therefore that $s = s_n$.

4·35. *Expansion of square roots.*

Theorem. Let $\alpha = \sqrt{\dfrac{r}{t}} > 1$ be irrational, then

$$\alpha = (s, \overline{s_1, \ldots, s_n}), \tag{1}$$

$$s_n = 2s, \qquad \text{and for } i = 1, \ldots, n-1 \tag{2}$$

$$s_i = s_{n-i} \tag{3}$$

hold. If conversely (1), (2) and (3) hold, then α is an irrational square-root > 1.

Proof. As $\alpha > 1$ and the number $\beta = -\alpha < 0$ is conjugate to α, it follows from the lemma that the complete fractions $\alpha_1, \alpha_2, \ldots$ of α are reduced, and therefore purely periodic. Hence α satisfies (1). As $\alpha = s + \dfrac{1}{\alpha_1}$ and $-\alpha = \beta = s + \dfrac{1}{\beta_1}$, α_1 and β_1 are conjugate.

$$\alpha_1 = (\overline{s_1, \ldots, s_n}). \tag{4}$$

Therefore it follows from the theorem of 4·32 that

$$-1 : \beta_1 = (\overline{s_n, \ldots, s_1}) \tag{5}$$

$$0 = \alpha + \beta = (s + \alpha) + 1 : \beta_1. \text{ Hence } -1 : \beta_1 = s + \alpha.$$

Therefore $$(\overline{s_n, \ldots, s_1}) = (2s, \overline{s_1, \ldots, s_n}) \tag{6}$$

holds. (6) implies (2) and (3). Conversely if α is defined by (1), (2) and (3), then (6) holds.

Let α_1 and β_1 be defined by (4) and (5), and let $\beta = s + 1 : \beta_1$, then it follows from (4) and (5) that α_1 and β_1 and therefore α, β are conjugate, and from (6) it follows that $\alpha + \beta = 0$. Hence α and β are the roots of a rational polynomial $tx^2 + 0x - r$. From $0 \neq s_n = 2s$, it follows that $s \geqq 1$, and therefore $\alpha > 1$, and as (1) is an infinite continued fraction, α must be irrational.

Corollary. Let $\alpha = \sqrt{(r : t)}$ and $P_1 : Q_1, \ldots$ be the convergents of α, then

$$t\, P_{kn}^2 - r\, Q_{kn}^2 = (-1)^{kn}\, t \tag{7}$$

holds for every $k = 1, 2, \ldots$.

Proof. Let $\alpha_1, \ldots$ be the complete fractions of α, then $\alpha_1 = \alpha_{1+kn}$

$$\alpha_{kn} = s_{kn} + \frac{1}{\alpha_{kn+1}} = 2s + \frac{1}{\alpha_1} = s + \alpha.$$

But, as $\alpha = \dfrac{P_{kn}\ \alpha_{kn} + P_{kn-1}}{Q_{kn}\ \alpha_{kn} + Q_{kn-1}}$,

$$\alpha = \frac{P_{kn}(s+\alpha) + P_{kn-1}}{Q_{kn}(s+\alpha) + Q_{kn-1}} \text{ holds ; hence}$$

$$Q_{kn}\ \alpha^2 - P_{kn}\ s - P_{kn-1} + \alpha\,(Q_{kn}\ s + Q_{kn-1} - P_{kn}) = 0.$$

As $\alpha^2 = r : t$ is rational, and α is irrational

$$\begin{aligned} P_{kn-1} + P_{kn}\ s - Q_{kn}\ r : t &= 0 \\ -P_{kn} + Q_{kn}\ s + Q_{kn-1} &= 0 \end{aligned}$$

hold. Multiply these equations with $Q_{kn}\,t$, and $-P_{kn}\,t$ respectively and add, then $tP_{kn}^2 - rQ_{kn}^2 + t(P_{kn-1}\,Q_{kn} - Q_{kn-1}\,P_{kn}) = 0$, whence (7) follows directly.

4·4. *Applications to theory of numbers.*

It is proposed to solve

$$ax - by = 1 \qquad (1)$$

by integral x and y.

Obviously (1) cannot be solved if there is a common factor of a and b different from ± 1. Therefore suppose a and b to be relatively prime. $a : b$ can be represented by an even continued fraction (see 4·21, theorem 1).

$a : b = (s_1, \ldots, s_{2m})$

$a : b = P_{2m} : Q_{2m}$, and as a and b are positive and relatively prime

$a = P_{2m}$, $b = Q_{2m}$, and therefore

$$a\,Q_{2m-1} - b\ P_{2m-1} = P_{2m}\ Q_{2m-1} - Q_{2m}\ P_{2m-1} = (-1)^{2m} = 1$$

holds. Hence one gets the integral solutions by

$$x = Q_{2m-1} + k\ b,$$

$$y = P_{2m-1} + k\ a, \qquad \text{where } k = 0, \pm 1, \pm 2, \ldots,$$

To solve by integral x and y,

$$x^2 - dy^2 = 1 \text{ (\textit{Pell's equation} †)}, \tag{2}$$

where d is a positive integral number.

From 4·35 it follows that $\sqrt{d} = \alpha = (s, \overline{s_1, \ldots, s_n})$; applying the corollary, it results that

$$P_{kn}^2 - d\,Q_{kn}^2 = (-1)^{kn}.$$

Therefore if n is even $\qquad (x, y) = (P_{kn}, Q_{kn})$

and if n is odd, $\qquad (x, y) = (P_{2kn}, Q_{2kn})$

are solutions for every positive integral k.

Example. $\qquad x^2 - 26\,y^2 = 1.$

$$\sqrt{26} = (5, \overline{10}) \qquad n = 1.$$

By this method one gets the solutions

$$\begin{aligned}(x, y) &= (P_2, Q_2) = (51, 10)\\ &= (P_4, Q_4) = (5201, 1020)\\ &= (P_6, Q_6) = (530451, 104030)\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

*4·5. *Continued fractions with elements* $\phi(x)$.

The general method of continued fractions, the elements of which have been given in 4·1, can be applied to different fields K. In 4·2 to 4·4, the field of the real numbers was chosen for K, and the expansion of a positive real number into a continued fraction with integral elements was studied. Thus the positive real numbers formed the system A, and the integral numbers formed the domain S mentioned in the general theory. The expansion of positive numbers into a continued fraction has furnished the opportunity for an approximation of real numbers by rational numbers. There arises the question now, whether in a similar manner, the power series in an indeterminate x^{-1} can be expanded into continued fractions with polynomials in x as their elements, and whether by this method the power series can be approximated by quotients of polynomials. "Approximation" always means that to a certain entity which is *to be approximated*, an infinite sequence of *approximating entities* is constructed such that the differences between the approximated and the approximating entities can be made as small as one likes. Thus an approximation implies that these differences are measurable, and a sequence approximating an entity may be made non-approximating when a different method of measuring the differences is used. In the theory which will be given here, the power series are measured by their "degrees" which are integral numbers; the measuring does not imply any consideration of convergence. The theory is therefore so general that nothing must be supposed about the field of the coefficients of the power series. On the other hand, this generality makes it necessary to define afresh the sum, the product etc. of power series. This definition must be done in such a manner that it tallies with the definition for the corresponding operation on polynomials for the case when only a finite number of coefficients is different from zero.

---

† Solved by Brahmagupta (born 598 A. D.) and independently by Fermat (1657). The name "Pell's equation" has no historical justification, but it is commonly used. (L. E. Dickson, History of the theory of numbers, Vol. II; B. B. Datta and A. N. Singh, History of Hindu Mathematics, Part II).

* May be omitted at a first reading.

4·51. *The field B.* Let F be an arbitrary field and x an indeterminate not included in F. The elements of F will be denoted by a, b, c, d, with or without indices. The elements of the ring $F[x]$ will be denoted by

$$f(x),\ g(x),\ \ldots \tag{1}$$

The integral domain $F[x]$ will be chosen as S.

In order to get a new system A, create new elements denoted by Greek letters

$$\varphi(x),\ \psi(x),\ \chi(x),\ \omega(x),\ \ldots \tag{2}$$

in the following manner:

$$\begin{aligned}\varphi(x) &= a_n\, x^n + a_{n-1}\, x^{n-1} + \ldots + a_0 + a_{-1}\, x^{-1} + \ldots + a_{-k}\, x^{-k} + \ldots \\ &= 0\, x^{n+m} + \ldots + 0\, x^{n+1} + a_n\, x^n + \ldots + a_{-k}\, x^{-k} + \ldots = \sum_{-\infty}^{n} a_k\, x^k. \end{aligned} \tag{3}$$

This purely formal definition means that to every sequence of coefficients from F with fixed decreasing integral indices

$$a_n,\ a_{n-1},\ \ldots$$

there corresponds one of the new elements, and this element will not be changed if one puts before a_n a finite set of null-coefficients. The addition and the multiplication of the elements (2) will be defined now in such a way that the elements (2) for which $a_k = 0$, for $k < 0$ form a subring isomorphic to $F[x]$.

Definition. Let $n \geqq m$, $\varphi(x) = \sum_{-\infty}^{n} a_k x^k$, $\psi(x) = \sum_{-\infty}^{m} b_k x^k = \sum_{-\infty}^{n} b_k x^k$, where $0 = b_{m+1} = \ldots = b_n$ if $n > m$; then

$$\varphi(x) + \psi(x) = \chi(x) = \sum_{-\infty}^{n} c_k x^k \text{ and}$$

$$\varphi(x)\,\psi(x) = \omega(x) = \sum_{-\infty}^{n+m} d_k x^k,$$

where $$c_k = a_k + b_k, \qquad d_k = \Sigma a_i b_{k-i} \tag{4}$$
$$n \geqq i \geqq k - m.$$

The definition is obviously independent of null-coefficients put before; the commutative, associative and distributive laws hold, and the subtraction is uniquely defined by

$$b_k = c_k - a_k.$$

Hence for the null-element every coefficient is 0. If for the coefficients of $\psi(x)$ the conditions $b_k = 0$, for $k \neq 0$ hold, then in $\varphi(x)\,\psi(x) = \Sigma\, d_k x_k$

$$d_k = b_0 a_k \qquad \text{holds.}$$

The elements (2) form a ring B and those elements for which $a_{k>0} = 0$ form a subring for which the addition and multiplication has been defined in the same way as for polynomials. Hence there is an isomorphism I by which this subring becomes isomorphic to $F[x]$. Let $\varphi(x) \neq 0$, then $\varphi(x)$ has at least one coefficient $\neq 0$, let n be the highest index of the non-vanishing coefficients, then

$$\varphi(x) = \sum_{-\infty}^{n} a_k x^k, \quad a_n \neq 0,$$

n is said to be the *degree* of $\varphi(x)$. From (4) follows directly:

The degree of a product is equal to the sum of the degrees of the factors.

The degree of a sum of elements of different degrees is equal to the maximum degree of the summands.

From this remark it follows that a product of two elements $\neq 0$ cannot be equal to 0. Hence the ring B is an integral domain. Now *identify* the elements of $F[x]$ with the corresponding elements (2). For polynomials

$\neq 0$ of $F[x]$, the degree tallies with that of the corresponding elements of B, but the zero-element, which is a polynomial of degree -1 in $F[x]$, has *no degree* when considered as an element of B.

The elements $\sum_{-\infty}^{n} b_k x^k$, $b_k = 0$, for $k \neq 0$ are identified with b_0, and

$b_0 \varphi(x) = \sum_{-\infty}^{k} b_0 a_k x^k$ holds. Let $\psi_k(x) = x^{-k} + 0\; x^{-k-1} + \dots$; then $x^k \psi_k(x) = 1$. Every field containing B contains the quotient field Q of $F[x]$. The elements of B, which are quotients of elements of $F[x]$ form a ring which is isomorphic to a subring of Q. The elements of this ring will therefore be identified with the corresponding elements of Q. So $\psi_k(x)$ is identified with x^{-k} and the *finite* sum $\sum_{-m}^{n} a_k x^k$ is identified with the *symbolic* sum $\varphi(x) = \sum_{-\infty}^{n} a_k x^k$, where $a_k = 0$, for $k < -m$.

Using these notations, one can extend the algorithmus of division of the polynomials to the elements of B.

Let $\varphi(x)$ and $\psi(x)$ be of degree n and m respectively, where $n \geqq m$, and a_n and b_m their highest coefficients,

$$\frac{a_n}{b_m} = c_{n-m},\quad \varphi_1(x) = \varphi(x) - c_{n-m}\, x^{n-m}\, \psi(x) \text{ is of degree } n_1 < m.$$

A repetition of this procedure furnishes

$$\varphi_2(x) = \varphi_1(x) - c_{n_1-m}\, x^{n_1-m}\, \psi(x) = \varphi(x) - (c_{n-m}\, x^{n-m} + c_{n_1-m}\, x^{n_1-m})\, \psi(x),$$

and by further repetitions one gets an enumerable set of elements c_k of F for $k \leqq n - m$, so that $\chi_\nu(x) = \sum_{n_\nu-m}^{n-m} c_k x^k$, and

$$\varphi_{\nu+1}(x) = \varphi(x) - \chi_\nu(x)\, \psi(x) \text{ is of degree } n_{\nu+1} < n_\nu.$$

Let $\chi(x) = \sum_{-\infty}^{n-m} c_k x^k = \chi_\nu(x) + \omega_\nu(x)$; then $\omega_\nu(x)$ is of degree $n_{\nu+1} - m$ and therefore $\psi(x)\omega_\nu(x)$ is of degree $n_{\nu+1}$. $\varphi(x) - \psi(x)\,\chi(x) = \varphi(x) - \psi(x)\,\chi_\nu(x) - \psi(x)\,\omega_\nu(x)$ is of degree $< n_\nu$ for every ν, hence this difference is 0. Hence $\varphi(x) = \psi(x)\,\chi(x)$ holds. As $\psi(x)$ was supposed to be an arbitrary element $\neq 0$ of B, it follows :

Theorem. The set B of the elements (2) is a field containing the quotient field Q of $F[x]$.

4·52. *Expansion of the elements of B into continued fractions.* The general theory of continued fractions which has been explained in 4·1 can be applied to the expansion of elements of the type $\phi(x)$ if the field B is taken for K, the domain $F[x]$ is taken for S, and the system of the elements with non-negative degree is taken for the system A. It is easy to prove that those elements satisfy the conditions required for elements of a system A (see 4·11). Of course, an element is of positive degree if and only if its inverse is of negative degree.

Now

$$\phi(x) = \sum_{-\infty}^{n} a_k\, x^k = \sum_{0}^{n} a_k\, x^k + \sum_{-\infty}^{-1} a_k\, x^k = f(x) + \phi_1(x).$$

Hence : Either $\phi(x) = f(x)$,

or $\phi(x) = f(x) + 1 : \psi(x)$, where $\text{degree}(\psi(x)) > 0$.

The representation (1) of $\phi(x)$ is uniquely determined. There exists therefore an expansion of $\phi(x)$ into a continued fraction. The first element $s_1 = f(x)$, may be of any degree $\geqq 0$ or it might be the zero-element, whereas the second element s_2 (if any) can be supposed to be of positive degree ; the same holds for $s_3, s_4, \ldots$. If one makes this supposition about the degrees, the expansion is uniquely determined. Hence

Theorem. The elements 4·51,(2) can be represented in one and only one manner by a continued fraction $(s_1, s_2, \ldots)$ where s_i is a polynomial in x, whose degree is > 0, for $i > 1$.

The degree of a polynomial s has just the properties of the function $N(s)$ in 4·12. From that section and the preceding theorem therefore results :

Corollary. The finite continued fractions represent the elements of Q and every element of Q is represented by a finite continued fraction.

4·53. *Approximation by rational functions.* The elements of B can be approximated by finite continued fractions whose elements are polynomials. The theory of approximation which will be given now, has much analogy with the approximation of real numbers by finite continued fractions with integral elements explained in 4·2 ; the same formulas of the general theory (see 4-1) will be applied. Whereas the real numbers have been approximated in such a way that the absolute value of the "error" was made smaller than any positive number, the elements of B will be approximated with an error whose *degree* diverges to $-\infty$. If the field F of the coefficients consists of numbers, the functions of x which are the elements of B are numerically approximated by the continued fractions for absolute values of x which are sufficiently high. Thus the method can be used for a numerical approximation of the asymptotic behaviour of those functions.

Let an element α_1 of B be expanded into a continued fraction $(s_1, s_2, \ldots)$ satisfying the conditions of the preceding theorem. Denote

$$\mathrm{d}_i = \text{degree } s_i, \quad \text{for } i = 1, 2, \ldots . \tag{1}$$

Hence $\mathrm{d}_1, \mathrm{d}_2, \ldots$ are positive integers. Apply the notations of 4-1 ; then it follows from $\alpha_i = s_i + I : \alpha_{i+1}$ that

$$\text{degree } \alpha_i = \mathrm{d}_i. \tag{2}$$

As furthermore $\alpha_i = a_i : a_{i+1}$, it follows that $a_2 = \alpha_2 a_3 = \alpha_2 \alpha_3 a_4 = \ldots = \alpha_2 \ldots \alpha_{k+1} a_{k+2}$, and therefore

$$\text{degree } (a_2 : a_{k+2}) = \mathrm{d}_2 + \ldots + \mathrm{d}_k + \mathrm{d}_{k+1}. \tag{3}$$

From the general formulas

$$\mathrm{Q}_1 = I,\ \mathrm{Q}_2 = s_2, \ldots \mathrm{Q}_i = s_i\ \mathrm{Q}_{i-1} + \mathrm{Q}_{i-2},$$

it follows that for $\mathrm{i} = 2, 3, \ldots$, Q_i has a positive degree. By mathematical induction, it follows that these degrees increase steadily with i, and in consequence

$$\begin{aligned} \text{degree } \mathrm{Q}_k &= \text{degree } (s_k\ \mathrm{Q}_{k-1}) = \mathrm{d}_k + \text{degree } \mathrm{Q}_{k-1} \\ &= \mathrm{d}_2 + \ldots + \mathrm{d}_k. \end{aligned} \tag{4}$$

Now

$$\alpha_1 - \frac{\mathrm{P}_k}{\mathrm{Q}_k} = \frac{(-1)^{k-1}}{a_2}\ \frac{a_{k+2}}{\mathrm{Q}_k}.$$

From this formula together with (3) and (4) it follows that

$$\text{degree } \left(\alpha_1 - \frac{\mathrm{P}_k}{\mathrm{Q}_k} \right) = -\,\mathrm{d}_{k+1} - 2 \text{ degree } \mathrm{Q}_k. \tag{5}$$

The right hand side of (5) can also be expressed by $-$degree $(Q_k Q_{k+1})$ and is therefore equal to degree $\left(\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}}\right)$. This shows that when α_1 is approximated by its k^{th} convergent, the degree of the error is the same as the degree of the difference between the k^{th} and the $(k+1)^{st}$ convergent. It is easy now to prove a theorem analogous to the theorem on the approximation of real numbers which has been established in 4·22.

Theorem. degree $\left(\alpha_1 - \frac{f(x)}{g(x)}\right) >$ degree $\left(\alpha_1 - \frac{P_k}{Q_k}\right)$ implies

$$\text{degree } g(x) > \text{degree } Q_k.$$

Proof. Put $\beta = \frac{f(x)}{g(x)} - \frac{P_k}{Q_k} = \left(\alpha_1 - \frac{P_k}{Q_k}\right) + \left(\frac{f(x)}{g(x)} - \alpha_1\right)$.

As β is the sum of two elements of B, where the first term has a higher degree than the second, its degree is the same as the degree of the first term, therefore it follows from (5) that

$$\text{degree } \beta = -\, d_{k+1} - 2 \text{ degree } Q_k. \tag{6}$$

On the other hand, $\beta g(x)\, Q_k$ is a polynomial in x and is different from zero. Hence

$$0 \leq \text{degree } (\beta g(x)\, Q_k) = \text{degree } \beta + \text{degree } g(x) + \text{degree } Q_k\,;$$

putting in the value of degree β given by (6), one gets

$$\text{degree } g(x) \geqq \text{degree } Q_k + d_{k+1} > \text{degree } Q_k.$$

Exercise

$$\tfrac{1}{2} \log \frac{x+1}{x-1} = x^{-1} + \tfrac{1}{3}x^{-3} + \tfrac{1}{5}x^{-5} + \cdots$$

Represent this function by a continued fraction and approximate it by rational functions.

4·54. *Continued fractions whose elements are polynomials.* To build up the theory of the expansion of the elements of B into continued fractions analogous to the corresponding theory for real numbers, it must be shown that every infinite continued fraction of the type considered here is indeed the expansion of an element of B. For this purpose the following lemma is helpful.

Lemma. Let $\alpha = (s_1, \ldots)$, $\alpha' = (s'_1, \ldots)$ be finite or infinite continued fractions; let m be the lowest index for which $s_m \neq s'_m$ holds, or for which s_m, but not s'_m exists, and let $(s_1, \ldots, s_m) = \mathrm{A}$, $(s'_1, \ldots, s'_m) = \mathrm{A}'$, then

$$\text{degree } (\alpha - \alpha') = \text{degree } (\mathrm{A} - \mathrm{A}') \text{ holds.} \tag{1}$$

Proof. Whithout loss of generality suppose that degree $s_m = \mathrm{r} \geqq$ degree $s'_m = \mathrm{r}'$. The ordinary notations will be used for the convergents of α, and those of α' will be distinguished by a dash.

Then
$$\mathrm{P}_i = \mathrm{P}'_i,\ \mathrm{Q}_i = \mathrm{Q}'_i \quad \text{for } \mathrm{i} < \mathrm{m};$$
$$\mathrm{Q}_m = s_m \mathrm{Q}_{m-1} + \mathrm{Q}_{m-2}, \qquad \text{degree } \mathrm{Q}_m = \mathrm{r} + \mathrm{q}$$
$$\mathrm{Q}'_m = s'_m \mathrm{Q}_{m-1} + \mathrm{Q}_{m-2}, \qquad \text{degree } \mathrm{Q}'_m = \mathrm{r}' + \mathrm{q}.$$

Now

$$\mathrm{A} - \mathrm{A}' = \left(\frac{\mathrm{P}_{m-1}}{\mathrm{Q}_{m-1}} + \frac{(-1)^m}{\mathrm{Q}_{m-1}\mathrm{Q}_m}\right) - \left(\frac{\mathrm{P}_{m-1}}{\mathrm{Q}_{m-1}} + \frac{(-1)^m}{\mathrm{Q}_{m-1}\mathrm{Q}'_m}\right)$$

$$= (-1)^m \frac{s'_m - s_m}{\mathrm{Q}_m \mathrm{Q}'_m}.$$

Two different cases have to be considered.

1. Let $\mathrm{r} = \mathrm{r}'$; as degree $(s'_m - s_m) \geqq 0$,

degree $(\mathrm{A} - \mathrm{A}') \geqq -2(\mathrm{r}' + \mathrm{q}) =$ degree $\dfrac{1}{\mathrm{Q}'^2_m}$.

2. Let $\mathrm{r} > \mathrm{r}'$; then degree $(s'_m - s_m) = \mathrm{r}$, and therefore

degree $(\mathrm{A} - \mathrm{A}') = \mathrm{r} - (\mathrm{r} + \mathrm{q} + \mathrm{r}' + \mathrm{q}) \geqq -2(\mathrm{r}' + \mathrm{q}) =$ degree $\dfrac{1}{\mathrm{Q}'^2_m}$.

Hence

$$\text{degree } (\mathrm{A} - \mathrm{A}') \geqq \text{degree } \frac{1}{\mathrm{Q}'^2_m}$$

holds in every case.

From (1) it follows that

degree $(\mathrm{A} - \alpha) =$ degree $\dfrac{1}{\mathrm{Q}_m \mathrm{Q}_{m+1}} <$ degree $\dfrac{1}{\mathrm{Q}^2_m} \leqq$ degree $\dfrac{1}{\mathrm{Q}'^2_m}$,

and that degree $(\mathrm{A}' - \alpha') =$ degree $\dfrac{1}{\mathrm{Q}'_m \mathrm{Q}'_{m+1}} <$ degree $\dfrac{1}{\mathrm{Q}'^2_m}$. Hence degree $(a - a')$ = degree $[(A - A') - (A - a) + (A' - a')]$ = degree $(A - A')$, as the degree of the first one of the three summands is greater than the degrees of the two other summands.

Theorem. Let $s_1, s_2, \ldots$ be an infinite set of polynomials of $F[x]$ and let for $i > 1$, degree $s > 0$, then there exists a continued fraction $(s_1, s_2, \ldots)$.

Proof. The set $s_1, s_2, \ldots$ determines uniquely the values $P_1, \ldots, Q_1, \ldots,$ and $P_N : Q_N = (s_1, \ldots, s_N)$. Let $1 < n < N$; from the preceding lemma it follows, that degree $(P_N : Q_N - P_n : Q_n)$ = degree $(P_{n-1} : Q_{n-1} - P_n : Q_n)$ = degree$\left(\dfrac{1}{Q_n\ Q_{n-1}}\right) = -k_n$, where k_n increases to infinity, with n.

$$P_N : Q_N = \sum_{-\infty}^{m} a_k x^k = \sum_{1-k_n}^{m} b_k x^k + \sum_{-\infty}^{k_n} c_k x^k.$$

The coefficients b_k are independent of N. As k_n increases with the index n, one gets an infinite set $b_m, \ldots, b_{-k_1}, \ldots$ determining

$$\varphi(x) = \sum_{-\infty}^{m} b_\nu x^\nu.$$

Finally one has to prove that $\varphi(x) = (s_1, s_2, \ldots)$. Let $\varphi(x) = (s'_1, s'_2, \ldots)$, and m be the smallest index for which $s_m \neq s'_m$, then it follows from the lemma that for every $n > m$,

$$\text{degree } (\varphi(x) - (s_1, \ldots, s_n)) = \text{degree } (\varphi(x) - (s_1, \ldots, s_m))$$

holds, as both the sides are equal to degree $((s'_1, \ldots, s'_m) - (s_1, \ldots, s_m))$.

But $\varphi(x) - (s_1, \ldots, s_n) = b_{-k_n} x^{-k_n} + b_{-k_n-1} x^{-k_n-1} + \ldots$ is of degree $-k_n$ which decreases infinitely with n. Thus there is no index like m; hence the theorem.

4·6. *Continued fractions with rational elements.*

Let S be the field of the rational numbers, then every finite continued fraction

$$(s_1, \ldots, s_n) = \frac{P_n}{Q_n} = \frac{P_1}{Q_1} + \left(\frac{P_2}{Q_2} - \frac{P_1}{Q_1}\right) + \ldots + \left(\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right) \tag{I}$$

$$= s_1 + \frac{1}{Q_1\ Q_2} - \ldots + \frac{(-1)^n}{Q_{n-1}\,Q_n}$$

represents a rational number, but an infinite continued fraction determines a number by approximation if and only if

$$\Sigma \frac{(-1)^n}{Q_{n-1}\, Q_n} \tag{2}$$

converges. If the sum (2) is convergent,

$$(s_1, s_2, \ldots) \tag{3}$$

determines a real number equal to (2). A necessary condition for the convergence of (3) is therefore

$$|Q_{n-1}\; Q_n| \longrightarrow \infty. \tag{4}$$

If the numbers Q_n are either > 0 each, or < 0 each, or of alternating sign, the sum (2) is an alternating sum ; hence in these cases the continued fraction converges if $|Q_n\; Q_{n-1}|$ increases steadily to infinity.

4·61. *Convergence of continued fractions*. For the continued fractions considered above, some criteria of convergence will be established now. In these investigations, every sequence (series, continued fraction) which does not converge to a real number will be called *divergent*.

Theorem 1. If $\Sigma|s_n|$ is convergent, 4·6, (3) is divergent.

Proof. At first, it will be shown by mathematical induction that

$$Q_n < \prod_1^n (1 + |s_j|). \tag{1}$$

As $Q_1 = 1$, $Q_2 = s_2$, the formula holds for $n < 3$. If (1) is true for $n < m$, if follows from

$$Q_m = s_m\, Q_{m-1} + Q_{m-2},$$

that

$$|Q_m| < \prod_1^{m-2} (1 + |s_j|).\;\; \{|s_m|(1 + |s_{m-1}|) + 1\} < \prod_1^m (1 + |s_j|).$$

If Σs_j converges, the infinite product $\Pi(1 + |s_j|)$ converges to a positive number Q, and $|Q_n| < Q$ holds for every index n. Hence 4·6, (4) does not hold and the continued fraction is divergent.

Let $s_j > 0$ for $j > 1$. From $Q_1 = 1$, $Q_2 = s_2 > 0$, $Q_n = s_n Q_{n-1} + Q_{n-2}$ it follows by mathematical induction that each number $Q_i > 0$.

$$Q_n Q_{n-1} = s_n Q_{n-1}^2 + Q_{n-1} Q_{n-2} > Q_{n-1} Q_{n-2} > 0.$$

4·6, (2) is therefore an alternating series, whose elements have steadily decreasing absolute values. This series converges therefore if and only if 4·6, (4) is satisfied. These considerations lead to the following theorem.

Theorem 2. Let $s_i > 0$ for $i > 1$, then the continued fraction 4·6, (3) is convergent if and only if Σs_i is divergent.

Proof. If $\Sigma s_i = \Sigma |s_i|$ is convergent, the continued fraction is divergent, as has been proved by the preceding theorem.

Let Σs_i be divergent, then $\Sigma s_i \to \infty$. As $Q_i > 0$, $Q_1 = 1$, and $Q_{2n+1} = s_{2n+1} Q_{2n} + Q_{2n+1}$, we get by mathematical induction that $Q_{2n+1} \geqq 1$. Hence $Q_{2n} = s_{2n} Q_{2n-1} + Q_{2n-2} \geqq s_{2n} + Q_{2n-2}$, and as $Q_2 = s_2$, it follows by mathematical induction that

$$Q_{2n} \geqq \sum_1^n s_{2j}. \tag{2}$$

If the sum (2) diverges with steadily increasing n,

$$Q_{2n-1} Q_{2n} \to \infty, \text{ and } Q_{2n} Q_{2n+1} \to \infty; \tag{3}$$

and therefore 4·6, (4) is satisfied. If however (2) converges, then Σs_{2j+1} diverges, and therefore $Q_{2n+1} \geqq s_2(s_3 + \ldots + s_{2n+1})$ diverges with increasing n. Thus 4·6,(4) holds in every case, and this condition implies the convergence of the continued fraction in the case considered here. Hence the theorem.

4·62. *Tests of irrationality.* The preceding investigations can be used to prove the irrationality of certain numbers.

Let $s_1 = 0$, $s \geqq 1$ for $i > 1$. As $\Sigma s_i \to \infty$ it follows from the preceding theorem that the continued fraction converges. The limit lies between the convergents with odd and those with even index, *i.e.* between $P_1 : Q_1 = 0$ and $P_2 : Q_2 = 1 : s_2$. It will be shown now that this value is *irrational*.

Let $\alpha_1 = (s_1, s_2, \ldots)$ be rational, say $\alpha_1 = \dfrac{a_2}{a_1}$, where a_1, a_2 are integral,

then $a_1 > a_2$ and $\dfrac{a_2}{a_1} = \dfrac{1}{s_2 + \alpha_2}$, hence $\alpha_2 = \dfrac{a_1}{a_2} - s_2 = \dfrac{a_3}{a_2}$, where $a_3 = a_1 - s_2 a_2$ is integral. As $\alpha_2 = (0, s_3, \ldots)$, there is $0 < \alpha_2 < 1$; hence $a_2 > a_3 > 0$. In the same manner, one gets

$$\alpha_2 = \frac{1}{s_2 + \alpha_3}, \ \alpha_3 = (0, s_4, \ldots) = \frac{a_4}{a_3} \text{ and } a_3 > a_4 > 0.$$

This procedure must end after a finite number of steps, as a sequence $a_1 > a_2 > a_3 > a_4 > \ldots$, of integral positive numbers cannot be continued indefinitely. Since the continued fraction has been supposed to be infinite, the assumption of α_1 to be rational leads to a contradiction. Hence α_1 is irrational.

Example. $s_1 = 0, s_2 = 2, s_3 = 1$, and for $m > 1$,

$$s_{2m} = \frac{2.\,4\,\ldots\,(2m-2)}{1.\,3\,\ldots\,(2m-3)} > 1, \ s_{2m+1} = \frac{3.\,5\,\ldots\,(2m-1)}{2.\,4\,\ldots\,(2m-2)} > 1;$$

then

$$Q_1 = 1, \ Q_2 = 2, \ Q_3 = 3,$$

and from the identities

$$\begin{aligned} 2\,.\,4\,\ldots\,2m &= 1\,.\,3\,\ldots\,(2m-1).\ s_{2m} + 2\,.\,4\,\ldots\,(2m-2) \\ 1\,.\,3\,\ldots\,(2m+1) &= 2\,.\,4\,\ldots\,2m.\ s_{2m+1} + 1\,.\,3\,\ldots\,(2m-1). \end{aligned}$$

it follows by mathematical induction that

$$Q_{2m} = 2\,.\,4\,\ldots\,2m, \ Q_{2m+1} = 1\,.\,3\,\ldots\,(2m+1),$$

hence

$$Q_n \ Q_{n-1} = n\,!\,;$$

thus the continued fraction is irrational. Its value is

$$\frac{1}{Q_1\,Q_2} - \frac{1}{Q_2\,Q_3} + \ldots + \frac{(-1)^n}{Q_{n-1}\,Q_n} + \ldots = \Sigma(-1)^n : n\,! = e^{-1}.$$

Hence e is irrational.

CHAPTER V

APPROXIMATION OF ROOTS

Introduction : Another dialogue.

Student. When I started reading Algebra, you advised me to study carefully the systems of linear equations ; so I did. I further read general algebra and continued fractions. At first it was hard work, but later on, I was quite successful.

Tutor. All right, but I don't think that you have met me for this. You are looking rather despondent.

St. Indeed. I am again in the wilderness.

T. Why ? Is there some difficulty in the book, which you want me to explain ?

St. It is not for that, but the whole subject became problematical to me again.

T. I wonder how.

St. Yesterday an engineer asked me to solve a certain algebraic equation. I replied that in consequence of the fundamental theorem of general algebra, there exist roots in a suitable extension of the field of the coefficients, and that for the fundamental theorem of classical algebra, this extension can be chosen as the field of the complex numbers. Thus there exist complex roots of the equation, and some of them might be real.

T. Was the engineer satisfied by your reply ?

St. Not at all ! He said that I seemed to be a great philosopher, and that I had missed the point completely. He was interested in real roots only, and he had no doubt about their existence. He has found out that the force (expressed in kilogrammes), acting on a certain part of an engine, was bound to satisfy that equation. He was asking me to compute that force, and nothing else.

T. And you could not ; the polynomial was too complicated.

St. It looked very simple. Something like $x^5 + 4x^3 + 2x + 6$. From Eisenstein's theorem it is irreducible, and therefore its real roots must be irrational; this I told the engineer.

T. Perhaps, the good man did not know anything about irrationality.

St. He did! but he was not at all interested in my statement. He said: "I don't want to have an infinity of decimals, even if you can provide me with them; compute the kilogrammes; I leave the grammes etc. to you!" Now for any positive x, the polynomial takes positive values only. So I told him that the real roots of the polynomial must be negative.

T. And, was this statement of any use to the engineer?

St. No, he knew already that the force was directed to the negative side, and then he said: "The direction of the force is not very interesting to me, as there is little difference whether the material is exposed to stress or to pressure; if you give me a solution with 30% of error and a wrong sign, I could make some use of it, but your philosophical talk is worth nothing." He was quite rude eventually.

T. And you?

St. I am bewildered. After having read about 200 pages of the book, I am still unable to solve a very simple algebraic problem, not even if 30% of error and a wrong sign are admitted! Though I got very interested in algebra, the engineer's argument has impressed me; I am afraid that all my hard work has been spent uselessly.

T. I rather think you have stopped reading at the wrong place. If you continue, you will be able to provide your friend with a solution which has considerably less than 30% of error.

St. I had already a glance on the next chapter, but I do not see any connection between its content and the preceding parts of the book, *e.g.* with general algebra, and then, there is another thing which strikes me: Every solution is given only approximately. I should like to know the solutions correctly. If for a particular application a few decimals only are requested, then I may neglect the higher terms of the correct result, but as a student of Pure Mathematics, I must know at first the proper solution before admitting some error for the sake of abbreviation.

T. How do you want to represent the solution if it happens to be an irrational number?

St. There are many ways of expressing irrational numbers. For instance, $\sqrt{2}$ is irrational ; it cannot be expressed as a ratio of two integers, but nevertheless $\sqrt{2}$ is a number. Everybody knows what is $\sqrt{2}$.

T. Suppose that I do not know it, and try to explain ?

St. $\sqrt{2}$ is the positive number, the square of which is equal to 2.

T. Well, I take it for granted that one and only one such positive number exists. Let x be positive and $x^2 = 2$, then $x = \sqrt{2}$, or $\sqrt{2}$ is the positive root of $x^2 - 2 = 0$. I think this statement is completely equivalent to yours.

St. It is.

T. You seem to be satisfied with this manner of expressing irrational numbers.

St. Of course, I am. If I could express the roots of every algebraic equation in a similar way, then there would be nothing to complain of.

T. My point is that in this case, the roots are expressed by a tautology.

St. I cannot follow you.

T. Listen, which are the roots of the polynomial $x^2 - 2$?

St. $\sqrt{2}$ and $-\sqrt{2}$.

T. Whereby $\sqrt{2}$ is nothing else than a symbol for the positive root of $x^2 - 2$ Besides the statement that $x^2 - 2$ has two real roots and that their sum is equal to zero, your solution of the problem to find the roots of $x^2 - 2$ is a mere tautology. Your conclusion goes like this : "Who is Amal ?". "The brother of Bimal". —"And who is Bimal ?". "Amal's brother." That means only that there exist two brothers Amal and Bimal, but it does not explain who is Amal.

St. But $\sqrt{2}$ is a well known number ; mathematicians have got used to it, and they calculate with $\sqrt{2}$ as they do with 23 or $1:7$. For me, there is no problem about $\sqrt{2}$.

T. Is it for the symbol $\sqrt{\ }$, that you hold this opinion ?

St. $\sqrt{\ }$ as a symbol is a mere convention ; the mathematicians could use any other notation instead of it, but I do not see any reason why symbols familiar to everybody should be replaced by new ones.

T. I fully agree with you, but for the sake of our conversation, let us denote the real roots of a polynomial $f(x)$, as far as they exist, by $[f(x)]_1$, $[f(x)]_2$, ..., $[f(x)]_n$ in their order of magnitude starting with the greatest root. Then your explanation of $\sqrt{2}$ means simply that $\sqrt{2}$ is equal to $[x^2 - 2]_1$.

St. Now you want me to admit that for every $f(x)$ which has a real, root, the symbol $[f(x)]_1$ must be considered as a solution of the equation $f(x) = 0$. You propose that there is no higher justification in considering $\sqrt{2}$ as a given number, than e.g. $[x^5 + 4x^3 + 2x + 6]_1$. But there is a huge difference between these two cases.

T. How that ?

St. We know more about $\sqrt{2}$ than that it is positive and that its square is equal to 2.

T. What do you know about $\sqrt{2}$?

St. $\sqrt{2} = 1.4142 \ldots$

T. 1.4142 is a rational number, whereas $\sqrt{2}$ is irrational.

St. Certainly, it is an infinite decimal fraction, but they have computed 200 decimals or even more of them. You cannot deny that $\sqrt{2}$ is very well known.

T. There still remains a certain error.

St. But a negligible one !

T. That depends on the purpose of the calculation. I was told that certain students of Pure Mathematics must know the proper solution before admitting some error for the sake of abbreviation.—Was it not so ?

St. But $\sqrt{2}$ is uniquely determined as the only positive root of $x^2 - 2$.

T. Yes, there exists one and only one such root. This is a statement on existence and on uniqueness, but nothing more than that. I think we have agreed already about this item. On the other hand, I admit that we know more than that about $\sqrt{2}$. For instance $\sqrt{2}$ is approximately equal to 1.4142, or to put it more clearly : $\sqrt{2}$ lies between 1.4142 and 1.4143. One can find out easily smaller intervals where $\sqrt{2}$ is situated ; there is no limit to the improvement of the approximation, and the diminution of the error. This "error" is not a kind of "mistake" which is the result of a negligent treatment ; on the contrary, it is an essential part of the solution of the problem. One cannot determine irrational numbers otherwise than approximately. This fact is concealed by some symbols we are using. Numbers represented by them are uniquely determined in the sense that there exists one and only one such number, but one cannot determine the place of an irrational number on the real axis otherwise than approximately.

St. Thus a formula like $(\sqrt[3]{14} + \sqrt{170})$ is only a "recipe" how to determine an irrational number approximately.

T. The formula denotes the greatest root of $x^6 - 28x^3 + 26$, and it shows of course a recipe how to compute that number approximately. A mental calculation furnishes 3 as a first approximation which could satisfy your friend completely.

St. Suppose, one could represent every root of a polynomial by the help of similar symbols ; this would furnish recipes to determine every root approximately.

T. As a matter of fact, not every root is representable in that manner, and even if it is, one prefers a different method sometimes.

St. My impression is that those methods have no connection with general algebra. Theory of approximation and general algebra apparently belong to different branches of Mathematics if not to two different Sciences.

T. They are complementary to each other. You already mentioned the two fundamental theorems which state the existence of roots in certain fields. They must be supplemented by investigations about *where* the roots ara situated in the field. The methods of investigation must tally with the structure of the particular field under consideration ; they cannot be of a general nature. The real numbers are ordered linearly, whereas the complex numbers correspond to the points of a plane. Hence one subdivides the real axis into intervals to determine real numbers, and similarly the plane is subdivided into certain domains (e.g. rectangular or circular ones) to locate complex numbers. Both ways lead to an approximate determination of numbers e.g. roots of a polynomial.

St. As the n roots of the polynomial $x^n + a_{n-1} x^{n-1} + \dots + a_0$ are uniquely determined by the numbers $a_0, \dots, a_{n-1}$, there must exist functions $f(a_0, \dots, a_{n-1})$ which show the distribution of the roots in the complex plane. One should investigate these functions ; this would be a worthy continuation of general algebra.

T. If you take "function" in the most general sense, there exist indeed such functions $f(a_0, \ldots, a_{n-1})$, e.g. the set of the roots itself is one. The problem is how to represent those functions; you should not expect that all of them are polynomials in $a_0, \ldots, a_{n-1}$. Every polynomial $x^n + a_{n-1} x^{n-1} + \ldots + a_0$ can be represented by a point $P = (a_0, \ldots, a_{n-1})$ of an n-dimensional space. There are theorems stating that if certain inequalities in $a_0, \ldots, a_{n-1}$ hold—*i.e.* if P is situated in a particular domain of the n-dimentional space—the n roots are distributed in the complex plane in a particular manner. These investigations are very interesting, but at the present time, the approximation of the roots is based more on the methods of calculation than on these theorems. In many cases, the theorems seem to be the result of the practice of calculation. For this reason, the author has started from Horner's scheme which gives the clue to the whole theory. I advise you to work out many numerical examples; it will help you to understand the theoretical portion.

5·1. *Horner's scheme.*

The theory of approximation of the roots of a polynomial $f(x)$ with real coefficients is based on the fact that $f(x)$ represents a continuous function if x is considered as a real variable. As a consequence, the function $f(x)$ takes all the values between $f(a)$ and $f(b)$ in the interval (a, b). In particular, if $f(a)$ and $f(b)$ have opposite signs, there must exist a root of $f(x)$ in this interval. This conclusion plays an important role in the approximation of the roots, but a theory of approximation based on it alone would involve an enormous amount of numerical calculations. A second important item is that

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \tag{1}$$

is the *Taylor expansion* of the function represented by it in the neighbourhood of $x = 0$. Hence

$$f(0) = a_0,\ f'(0) = a_1,\ \ldots,\ \frac{1}{n!} f^{(n)}(0) = a_n. \tag{2}$$

Thus one knows from (1) at the first sight much more about the behaviour of the function near $x = 0$ than in the neighbourhood of any other value. It is therefore a matter of the greatest importance to have a scheme for a quick calculation of the Taylor expansion at any point $x = q$, say

$$f(x) = a'_0 + a''_1(x - q) + \ldots + a^{(n)}_{n-1} (x - q)^{n-1} + a^{(n+1)}_n (x - q)^n.$$

The scheme which is used for this purpose is called *Horner's scheme* ; though it is very elementary, it discloses much about the function represented by $f(x)$. The coefficients $a'_0, a''_1, \ldots, a^{n+1}_n$ are continuous functions of q. For instance $a'_0 = f(q)$, and $a^{n+1}_n = a_n$ is a constant number. It is characteristic for the applications of Horner's scheme, that not a'_0 alone, but the full set of the coefficients and their interconnections are considered. Although Horner's scheme is mostly applied to real numbers, it can also be used when the coefficients belong to any field (or even to an arbitrary commutative ring) K.

5·11. *Expansion of $f(x)$ as a polynomial* in $x - q$. Let K be an arbitrary field, *e.g.* the field of the real numbers or of the complex numbers, q be an element of K and $f(x)$ a polynomial of $K[x]$.

$$f(x) = \sum_{0}^{n} a_i\, x^i = (x - q) \sum_{1}^{n} a'_k\, x^{k-1} + a'_0 = (x - q)\, f_1(x) + a'_0,$$

where $\qquad a_i = a'_i - q\, a'_{i+1}, \quad$ for $i = 1, \ldots, n - 1$, and

$$a'_n = a_n.$$

Hence $\qquad a'_{n-1} = a_{n-1} + qa'_n$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$a'_0 = a_0 + qa'_1.$$

Arrange the calculation of the coefficients a' as follows :

a_n	a_{n-1}	a_{n-2}	$\ldots\ a_1$	a_0
	qa'_n	qa'_{n-1}	$\ldots\ qa'_2$	qa'_1
a'_n	a'_{n-1}	a'_{n-2}	a'_1	a'_0

By the same method, $f_{11}(x) = \sum_{2}^{n} a''_k\, x^{k-2}$ is found out satisfying

$$f_1(x) = (x - q)\, f_{11}(x) + a''_1.$$

After $n - 1$ steps $f(x)$ is represented as a polynomial in $x - q$

$$f(x) = a'_0 + a''_1(x - q) + \ldots + a^{(n)}_{n-1}(x - q)^{n-1} + a_n(x - q)^n.$$

The complete *Horner's scheme* to get the Taylor expansion at $x = q$, looks like the following example.

Example. $f(x) = x^4 - 15x^3 + 68x^2 - 119x + 67$.

$$
q = 1. \qquad
\begin{array}{rrrrr}
1 & -15 & 68 & -119 & 67 \\
 & 1 & -14 & 54 & -65 \\
\hline
1 & -14 & 54 & -65 & 2 \\
 & 1 & -13 & 41 & \\
\cline{1-4}
1 & -13 & 41 & -24 & \\
 & 1 & -12 & & \\
\cline{1-3}
1 & -12 & 29 & & \\
 & 1 & & & \\
\cline{1-2}
1 & -11 & & &
\end{array}
$$

The lines of this scheme correspond to the consecutive steps. Their significance is as follows :

$$
\begin{aligned}
f(x) &= (x^3 - 14x^2 + 54x - 65)(x-1) + 2 \\
&= (x^2 - 13x + 41)(x-1)^2 - 24(x-1) + 2 \\
&= (x - 12)(x-1)^3 + 29(x-1)^2 - 24(x-1) + 2 \\
&= (x-1)^4 - 11(x-1)^3 + 29(x-1)^2 - 24(x-1) + 2.
\end{aligned}
$$

5·12. *Approximate calculation of roots by Horner's scheme.* Horner's scheme is very useful for calculating the roots. The method will be explained by the help of the above example.. Put $x = y + 1$, then

$$
\begin{aligned}
&f(x) = g(y) = y^4 - 11y^3 + 29y^2 - 24y + 2, \\
&f(1) = g(0) = 2, \\
&f'(1) = g'(0) = -24.
\end{aligned}
$$

Thus $f(x)$ has decreased from the value 67 at $x = 0$ to the value 2 at $x = 1$, and it is still decreasing as is seen from the value of the derivative. For this reason, one may expect that there is a root of $f(x)$ near $x = 1$. In the neighbourhood of $x = 1$, the function can be represented approximately by its two lowest terms. Applying the notation $\sim$ for approximation, one gets $f(x) \sim -24y + 2$ and therefore $f(x) = 0$ for $y \sim 0.1$. Thus it is helpful to represent $g(y)$ by a polynomial in $y - 0.1 = x - 1.1$.

$q = 0.1,$

$$
\begin{array}{lllll}
1 & -11 & 29 & -24 & 2 \\
 & +\ 0.1 & -\ 1.09 & +\ 2.791 & -2.1209 \\
\hline
1 & -10.9 & 27.91 & -21.209 & -0.1209 \\
 & +\ 0.1 & -\ 1.08 & +\ 2.683 & \\
\cline{1-4}
1 & -10.8 & 26.83 & -18.526 & \\
 & +\ 0.1 & -\ 1.07 & & \\
\cline{1-3}
1 & -10.7 & 25.76 & & \\
 & +\ 0.1 & & & \\
\cline{1-2}
1 & -10.6 & & &
\end{array}
$$

As $f(1.1) = -\ 0.1209 < 0$, there is a root between 1 and 1.1. One approximates therefore $f(x)$ by $-\ 18.526\ (x - 1.1) - 0.1209$, hence $x - 1.1 \sim -\ 0.007$. Thus, apply again Horner's scheme:

$q = -\ 0.007,$

$$
\begin{array}{lllll}
1 & -10.6 & 25.76 & -18.526 & -0.1209 \\
 & -\ 0.007 & +0.074249 & -\ 0.180839743 & +0.130947878201 \\
\hline
1 & -10.607 & 25.834249 & -18.706839743 & 0.010047878201 \\
 & -\ 0.007 & +0.074298 & -\ 0.181359829 & \\
\cline{1-4}
1 & -10.614 & 25.908547 & -18.888199572 & \\
 & -\ 0.007 & +0.074347 & & \\
\cline{1-3}
1 & -10.621 & 25.982894 & & \\
 & -\ 0.007 & & & \\
\cline{1-2}
1 & -10.628 & & &
\end{array}
$$

Hence the root is approximately equal to 1.093. The next approximation is $q = 0.00053$. By continuing in exactly the same manner, the calculation would become very burdensome. The number of the decimals to be considered increases at every step. On the other hand, the influence of the higher terms decreases with q. One can therefore omit those digits which are not influencing the terms required in the final result. It is convenient to state at the very beginning of the calculation, the error which is admissible. In the present problem, one obtains an approximation of the root, correct up to seven figures of decimals by the following consideration.

$18.888199572q = 0.010047878201 + 25.982894q^2 - 10.628q^3 + q^4$. As $q \sim 5.3.10^{-4}$, the two last terms will influence only the 9th and the following decimals on the right side for $5.310^{-4} < q < 5.4.10^{-4}$ the quadratic term becomes 0.000007 ....

Hence

$$q = 0.0005324, \qquad x = 1.0935324.$$

In this manner the approximation of the root can be improved gradually.

5·13. *A modification of Horner's scheme.* To get a first approximation of the roots, it is often important to get a quick and simple review of the values of the function for different values of x. For this purpose, the following modification of Horner's scheme is sometimes helpful.

Given $q_1, q_2, \ldots, q_{m<n}$, calculate by Horner's scheme :

$$f(x) = b_1 + (x - q_1)\ f_1(x) \qquad f(q_1) = b_1$$

$$f_1(x) = b_2 + (x = - q_2)\ f_2(x) \qquad f(q_2) = b_1 + (q_2 - q_1)b_2$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$f_{m-1}(x) = b_m + (x - q_m)\ f_m(x)$$

$$f(x) = b_1 + b_2(x-q_1) + b_3(x-q_2)\ (x-q_2) + \ldots + b_m(x-q_1) \ldots (x-q_{m-1}) + (x - q_1) \ldots (x - q_m)\ f_m(x).$$

To explain the method by an example, expand the polynomial considered in the previous example in this manner.

$q = 1$,	1	−15	68	−119	67
		1	−14	54	−65
$q = 2$,	1	−14	54	− 65	2
		2	−24	60	
$q = 3$,	1	−12	30	−5	
		3	−27		
	1	−9	3		

$$f(x) = 2 - 5(x - 1) + 3(x - 1)(x - 2) + (x - 1)(x - 2)(x - 3)(x - 9)$$

$$f(0) = 67,\ f(1) = 2,\ f(2) = -3,\ f(3) = -2,\ f(9) = 2 + 8(-5+21) = 130.$$

This representation shows that for $x<1$, $f(x)>0$, since each of the terms is >0, and that for $x>9$, $f(x)<0$, the 1st, the 4th and the sum of the two other terms being >9. So all roots are situated in the interval $(1, 9)$. We have alrady calculated one root in the interval $(1, 2)$; furthermore there is at least one root in the interval $(3, 9)$. $f(8) = -117$. Hence there is a root in the interval $(8, 9)$. The reader may calculate it by Horner's scheme as an *exercise*.

5·14. *Lagrange's method.* A different method for computing the roots will now be explained, and will be applied to the above example. If $f(x) = \sum\limits_0^n a_k\ x^k = 0$, then $\dfrac{1}{x}$ satisfies the condition $\sum\limits_0^n a_{n-k}\left(\dfrac{1}{x}\right)^k = 0$, and to every root x in the interval $(0, 1)$ there corresponds a value of $\dfrac{1}{x} > 1$. These considerations lead to the following method of approximation due to *Lagrange*.

If ξ is a root of $g(x)$, $a < \xi < a+1 = a + \dfrac{1}{x}$, $g(x) = f(a-x) = g_1\left(\dfrac{1}{a-x}\right)$; $\eta_1 > 1$ is a root of g_1, and $b \leq \eta_1 < b+1$, $\eta_1 = b + \dfrac{1}{\eta_2}$. By repetition of this procedure a representation of ξ as a continued fraction is obtained. By repeating the calculation, after n steps one gets the approximation $\dfrac{P_n}{Q_n}$ with an error

$$\left|\xi - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n\ Q_{n+1}} < \frac{1}{Q_n^2}.$$

This method will be illustrated by the example used beforehand. It is known that $x^4 - 15x^3 + 68x^2 - 119x + 67$ has a root in the interval $(8, 9)$. Therefore we represent this polynomial by Horner's method as a polynomial in $x - 8$.

$q = 8$,	1	−15	68	−119	67
		8	−56	96	−184
	1	−7	12	−23	−117
		8	8	160	
	1	1	20	137	
		8	72		
	1	9	92		
		8			
	1	17			

Hence $117\ \eta^4_1 - 137\ \eta_1^3 - 92\ \eta_1^2 - 17\ \eta_1 - 1 = 0$.

By mental arithmetic it is seen that for $q = 2$ the last coefficient is positive, but for $q = 1$ it must be negative, so η lies in the interval (1, 2), and one has to arrange for the Horner expansion for $q = 1$.

$q = 1$,	117	−137	−92	−17	−1
		117	−20	−112	−129
	117	−20	−112	−129	−130
		117	97	−15	
	117	97	−15	−144	
		117	214		
	117	214	199		
		117			
	117	331			

In the same manner as it has been done for η_1, one proves that η_2 is situated in the interval (1, 2).

$q = 1$,	130	144	−199	−331	−117
		130	274	75	−256
	130	274	75	−256	−373
		130	404	479	
	130	404	479	223	
		130	534		
	130	534	1013		
		130			
	130	664			

η_3 lies in the interval (2, 3).

$q = 2$,	373	−223	−1013	−664	−130
		746	1046	66	−1196
	373	523	33	−598	−1326
		746	2538	5142	
	373	1269	2571	4544	
		746	4030		
	373	2015	6601		
		746			
	373	2761			

Probably, the reader has by now got the experience that q must be chosen in such a way that the sign of the last coefficient does not change, but that the procedure adopted for $q+1$ would alter this sign; $q = 4$ will alter the sign of the second coefficient in the second main row of Horner's scheme, but the third coefficient will not change its sign, 6601 being too big. Hence the following coefficients will increase and therefore will not be negative. However for $q = 5$, -6601 is counterbalanced by more than 3000, and therefore -2761 by more than 12000, and so the sign of the last coefficient would be altered. Hence $q = 4$.

$q = 4$	1326	-4544	-6601	-2761	-373
		5304	3040	-14244	-68020
	1326	760	-3561	-17005	-68393
		5304	24256	82780	
	1326	6064	20695	65775	
		5304	45472		
	1326	11368	66167		
		5304			
	1326	16672			

At the next step, one gets $q = 1$. Hence $\xi = (8, 1, 1, 2, 4, 1, \ldots)$.

$P_1 = 8$	$Q_1 = 1$
$P_2 = 9$	$Q_2 = 1$
$P_3 = 17$	$Q_3 = 2$
$P_4 = 43$	$Q_4 = 5$
$P_5 = 189$	$Q_5 = 22$
$P_6 = 232$	$Q_6 = 27$
	$Q_7 \geqq 49.$

Hence $\xi \sim \dfrac{232}{27}$, the error $\dfrac{232}{27} - \xi$ is positive and $\leqq \dfrac{1}{27.49} = 0.00075\ldots$

As $\dfrac{232}{27} = 8.5925\ldots$, the value of ξ is correct up to the second decimal only; the third decimal may be 2 or 1. From this example it appears that Lagrange's method is sometimes slower than the method of 5·12. By practical experience, one learns best to find out the most convenient combination of methods in any particular case.

5-15. *Kakeya's theorem.* In 5-11 to 5-14, Horner's scheme has been used for calculating the real roots of equations with real coefficients. But the scheme can be applied—as has been stated at the beginning of this section—for arbitrary fields. It will be used now to find out a theorem on complex numbers. Let $b_0,\ b_1 + b_0,\ \ldots,\ b_n + \ldots + b_0$, be the coefficients of a polynomial. Put $q = \alpha$; then the first line of Horner's scheme is the following one :

$$\begin{array}{lllcl}
b_0 & b_1 + b_0 & b_2 + b_1 + b_0 & \cdot\cdot & b_n + b_{n-1} + \ldots + b_0 \\
 & \alpha b_0 & \alpha b_1 + (\alpha + \alpha^2) b_0 & & \alpha b_{n-1} + \ldots \Sigma \alpha^i b_0 \\
\hline
b_0 & b_1 + & b_2 + (1 + \alpha) b_1 + & \cdot\cdot & \dfrac{b_n(1 - \alpha) + \ldots + b_0(1 - \alpha^{n+1})}{1 - \alpha} \\
 & (1 + \alpha) b_0 & (1 + \alpha + \alpha^2) b_0 & &
\end{array}$$

Hence if α is a root, $\sum\limits_0^n b_k = \sum\limits_0^n b_k \alpha^{n+1-k}$ holds. Let b_k be positive numbers and α complex, then

$$\sum_0^n b_k \leqq \sum_0^n b_k \ |\alpha|^{n+1-k}. \tag{1}$$

If $|\alpha| < 1$, then $\sum\limits_0^n b_k < \sum\limits_0^n b_k \ |\alpha|^{n+1-k}$; hence (1) cannot be satisfied in this case. The absolute value of a root therefore cannot be smaller than 1. If $|\alpha| = 1$, then $\alpha = e^{\theta i}$, and $\Sigma\, b_k\, \alpha^{n+1-k} = \Sigma\, b_k \cos\,(x + 1 - k)\,\theta + i\,\Sigma\, b_k \sin\,(n + 1 - k) \neq \Sigma b_k$, when the numbers b_k are positive, unless $\theta = 2k\pi$, but $\alpha = 1$ cannot be a root, since no positive number satisfies an equation when all the coefficients are positive ; hence $|\alpha| > 1$. If therefore in $a_0\, y^n + a_1\, y^{n-1} + \ldots + a_n$

$$0 < a_0 < a < \ldots a_n, \tag{2}$$

then for every root α of this polynomial $|\alpha| > 1$ holds. Hence if $y = \dfrac{1}{x}$, the roots β of $\Sigma a_k\, x^k$ satisfy $|\beta| < 1$. This theorem is known as Kakeya's theorem.

Kakeya's theorem. The complex roots of $\Sigma\, a_k\, x^k$ have all absolute values < 1, if the coefficients satisfy (2).

5-20. *The roots of real polynomials.*

In this section

$$a,\ \ b,\ \ c,\ \ d,\ \ e, \tag{1}$$

—with or without indices and dashes—denote real numbers, in the same manner

$$\alpha, \ \beta, \ \gamma, \ \delta \tag{2}$$

denote complex numbers, and $\bar{\alpha}$ denotes the conjugate of α.

Hence $\alpha + \bar{\alpha}$ is real ; $\alpha\,\bar{\alpha}$ is non-negative ; $\alpha - \bar{\alpha} = ci$.

$$f(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + x^n \tag{3}$$

can be represented by
$$f(x) = \prod_{1}^{n} (x - \alpha_k). \tag{4}$$

5·21. *Real and complex roots.*

Theorem. If α is a root of a polynomial $f(x)$ with real coefficients, $\bar{\alpha}$ is also a root of it.

1st Proof. Let K be the field of real numbers, i and $-i$ be the roots of $x^2 + 1$, then $K(i) = K(-i)$ is the field of the complex numbers and there is an authomorphism J of this field interchanging i with $-i$ and leaving the real numbers unaltered. $f(x)$ will not be altered by J, hence α will be transformed into a root of $f(x)$, but as α will be transformed into $\bar{\alpha}$, the theorem is true.

2nd Proof. If α is real, $\bar{\alpha} = \alpha$. If α is not real, $(x - \alpha)(x - \bar{\alpha}) = g(x)$ is a real polynomial and irreducible in the field of the real numbers. As $f(x)$ and $g(x)$ have a common root, these polynomials have a common factor of positive degree. Hence $f(x)$ is divisible by $g(x)$ and $\bar{\alpha}$ is therefore a root of $f(x)$.

Corollary 1.

$$f(x) = (x - c_1) \dots (x - c_r).(x - \alpha_1)(x - \bar{\alpha}_1) \dots (x - \alpha_k)(x - \bar{\alpha}_k), \tag{1}$$

where $n = r + 2k$.

Corollary 2. If every root of $f(x)$ is counted as many times as its order of multiplicity in (1), the number of the real roots is $\equiv n \pmod{2}$.

Corollary 3. If n is odd, there exists at least one real root.

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2 = F(\alpha_1, \dots, \alpha_n) \tag{2}$$

is called the *discriminant* of $f(x)$. As F is a symmetric polynomial in $\alpha_1, \ldots, \alpha_n$ with integral coefficients, it follows (see p.144) that

$$\Delta = g(a_1, \ldots, a_n), \tag{3}$$

where g is a polynomial with integral coefficients. From (2) it follows that

$$\Delta = 0 \quad \text{if and only if } \alpha_i = \alpha_j \text{ for } i \neq j. \tag{4}$$

Let the n roots α_j be all different. As has been proved in 3-35, p. 146,

$$\Delta = \delta^2, \; \delta = \begin{vmatrix} \alpha_1^{n-1} & \ldots & \alpha_1 & 1 \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_n^{n-1} & \ldots & \alpha_n & 1 \end{vmatrix} \tag{5}$$

To get the conjugate of δ, we have to interchange every number in (5) with its conjugate. From (1) it follows that this operation means k interchanges of rows in the determinant (5). Now the product of two conjugate numbers is their "norm" N, which is a non-negative real number (see 3-32, p. 131). Thus

$$(-1)^k \, \Delta = (-1)^k \, \delta^2 = N(\delta) \geqq 0.$$

Hence the following theorem holds.

Theorem. Let $f(x)$ of degree n have n different roots. Then the discriminant of $f(x)$ is positive (negative) when the number of pairs of conjugate non-real roots is even (odd).

Corollaries. A real polynomial of degree 3 has three real roots if and only if the discriminant is positive.

A real polynomial of degree 4 with positive discriminant has either four different real roots or two pairs of conjugate complex roots.

Exercise. Prove the preceding theorem without the help of (4).

5-22. *Changes of sign.* At the beginning of 5-1, it has been mentioned already that if $a < b$, and the signs of $f(a)$ and $f(b)$ are different, then there is a root of $f(x)$ in the interval (a, b). This statement which is fundamental for the calculation of the real roots, must be complemented by two other statements (well known from the elements of Analysis) which show the interconnection of the roots of a real function with those of its derivative.

1. If $a < b$, and $f(a) = f(b)$, then there exists a root of $f'(x)$ in the interval (a, b).

2. If $f(x) = (x - \alpha)^k \, g(x)$, $g(\alpha) \neq 0$, $k > 0$, then

$f'(x) = (x - \alpha)^{k-1} \, g_1(x)$, where $g_1(\alpha) \neq 0$, since $g_1(x) = k\,g(x) + (x - \alpha)\,g'(x)$.

Therefore, if the roots of $f(x)$ take m different real values $\alpha_1, \ldots, \alpha_m$, there exists at least one root of $f'(x)$ in each of the $m - 1$ different intervals (α_i, α_{i+1}). If α_k is a multiple root with the multiplicity $q + 1$, it can be considered as a set of q degenerate intervals, each of them containing exactly one root of $f'(x)$. $f(x)$ has the same sign at every point of an interval; in two consecutive intervals (α_{i-1}, α_i) and (α_i, α_{i+1}) the sign of $f(x)$ is different, when α_i is a simple root or a multiple root of an odd order; the sign is not different if α_i is a multiple root of even order. Thus if α_k is a multiple root of order $q + 1$ of $f(x)$, it is a multiple root of order q of $f'(x)$.

These properties hold for every analytic function with a finite number of roots, and are not special properties of polynomials. If the coefficients of $f(x)$ are all positive (all negative), $f(x)$ is obviously positive (negative) for every positive value of x. Hence $f(x)$ has no positive roots when there is no change of the sign in the sequence of the coefficients of $f(x)$. So we are led to study the connection between the existence of roots and the signs of the coefficients. The experience got by using Horner's scheme will be very helpful.

Expand $f(x)$ as a polynomial in $x-b$

$$f(x) = f_b(x - b) = a_{b,n} \, (x - b)^n + \ldots + a_{b,0}. \tag{1}$$

Given $f(x)$ and any real number b, then a set of $n + 1$ real numbers $a_{b,n}$, $a_{b,n-1}$, …, $a_{b,0}$ is uniquely determined; of these, $a_{b,n} = a_n$ independent of b and

$$a_{b,0} = f(b).$$

Hence $a_{b,0} = 0$ if and only if b is a real root of $f(x)$, and for $0 < k < n$

$$a_{b,k} = \frac{1}{k!} \, f^{k}(b). \tag{2}$$

Consider now the *changes* of sign in the sequence

$$a_{b,n}, \; a_{b,n-1}, \; \ldots, \; a_{b,0}. \tag{3}$$

To determine uniquely the number of these changes, it is necessary to give some sign to those coefficients which are equal to zero. Whithout loss of generality, suppose that $a_n \neq 0$; if any coefficient, or any set of consecutive coefficients which are equal to zero, follow in (3) immediately after a positive (negative) coefficient, they will be considered to be positive (negative) themselves. By this rule, to every element of (3) a uniquely determined sign is allotted. E.g. when $f(x) = x^8 - 3x^5 + 7x^3 + 6x^2 - 1$ and $b = 0$, the sequence (3) is :

$$1 \quad 0 \quad 0 \quad -3 \quad 0 \quad 7 \quad 6 \quad 0 \quad -1 \quad \text{and the signs are}$$

therefore : $+ + + - \quad - + + + - .$

The number of changes of sign in (3) is not altered when from any set of consecutive equal signs, the first only is considered, and the other ones are struck out ; hence one gets the same number of changes if the zero-coefficients are simply struck out, but it is convenient to allot a uniquely determined sign to every element of the sequence (3).

Given $f(x)$, the number of changes will be considered now as a function $C(b)$ of b. Then

$$0 \leqq C(b) \leqq n. \tag{4}$$

If the first and the last element of the sequence (3) have the same sign, $C(b)$ is an even number ; if they have different signs, $C(b)$ is odd. Hence $C(b)$ is even when $a_n\, f(b) > 0$, and it is odd when $a_n\, f(b) < 0$.

5·221. *Alterations of the first and the second kind.* To investigate $C(b)$ as a function of b, it is not necessary to consider the sequence of the coefficients $a_{b,m}$ (for $m = n, \ldots, 1, 0$) themselves ; it suffices to examine the sequence

$$\pm \cdots + \cdots - \cdots \pm \tag{1}$$

of the *signs* of these $n + 1$ coefficients. A few general remarks on the alterations of any sequence (1) generated by transforming signs + into −, or conversely will be helpful ; one can restrict the consideration to such alterrations where the first sign remains unchanged, since the first coefficient of the polynomial is constant for all the values of b.

Every alteration of the sequence (1) which does not change the first sign can be generated by the help of at most n alterations done one after the other one, and each changing one sign only. An alteration which changes the second, third, …, $(n + 1)^{st}$ sign either makes that sign equal to the preceding one—then it will be called an alteration of the *first* kind, or it makes it different from the preceding sign — then it is of the *second* kind.

Lemma. An alteration of the first kind either diminishes the number of changes in (1) by one or two, or it leaves them unaltered ; the diminution by one takes place if and only if the last sign of (1) is altered.

Proof. If the last sign of (1) is altered by an alteration of the first kind, then the last two signs were different before the alteration, and are made equal by it ; hence one change is lost, whereas the other changes are preserved, and no new change is created. If the sign to be altered is not the last one, then it is the middle of a triplet of signs in which the two first signs are different. One has therefore to consider the following four cases (the arrows denoting the alteration) :

$$+ \; - \; - \;\rightarrow\; + \; + \; - \,, \qquad - \; + \; + \;\rightarrow\; - \; - \; +$$

$$+ \; - \; + \;\rightarrow\; + \; + \; + \,, \qquad - \; + \; - \;\rightarrow\; - \; - \; -$$

In the two first cases, the number of changes is unaltered, in the third and the fourth case, two changes are lost. Hence the lemma.

Corollary 1. If an alteration A is composed of alterations of the first kind only, the number of changes either decreases or it remains unaltered ; if in particular the last sign is unaltered by A, the number of the lost changes is an even non-negative number.

Proof. As by no alteration of the first kind a change can be "gained" no change can be gained by A. Suppose now that the last sign is unaltered by A. Of the alterations of the first kind composing A, let there be s alterations losing one change, and t alterations losing two changes. As those s alterations are the only ones where the last sign is altered, s is even, say $s = 2k$; the number of changes lost by A is equal to $2k + 2t$.

Corollary. 2. If A is composed of alterations of the first kind, and the r first signs of (1) are equal, then they remain equal when A is performed. Conversely, if A' is composed of alterations of the second kind and the r first signs are alternately + and −, then they remain so when A' is performed.

Proof. The statements hold obviously for alterations of the first (the second) kind, and therefore for alterations A (alterations A').

Exercises : Show that an alteration composed of alterations of the first kind only can also be generated by composing alterations of the first and of the second kind.

Prove that an alteration composed of one or more alterations of the first kind cannot be generated by composing alterations of the second kind only (and conversely).

5·222. *Monotony of* $C(b)$. The results of 5·221 will now be applied to investigate $C(b)$ when b runs over the real axis. Consider two different values of b, say b_1 and $b_2 = b_1 + q$, where $q > 0$. Let $F(\xi)$ be any polynomial of degree n in the real variable ξ with real coefficients. Put

$$\begin{aligned} \xi - b = x,\ F(\xi) = f(x) &= a_n\, x^n + a_{n-1}\, x^{n-1} + \ldots + a_0 = \varphi(x - q) \\ &= a_n\, (x - q)^n + a^{(n)}{}_{n-1}(x - q)^{n-1} + \ldots + a'_0 \end{aligned} \tag{2}$$

The coefficients of $\varphi(x - q)$ are obtained by Horner's scheme, the different steps of the scheme being the following ones:

$$\begin{array}{lllll} a_n, & a_{n-1}, & \ldots, a_2, & a_1, & a_0 \\ a_n, & a'_{n-1}, & \ldots, a'_2, & a'_1, & a'_0 \\ a_n, & a''_{n-1}, & \ldots, a''_2, & a''_1, & a'_0 \\ a_n, & a'''_{n-1}, & \ldots, a'''_2, & a''_1, & a'_0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_n, & a^{(n)}{}_{n-1}, & \ldots, a'''_2, & a''_1, & a'_0. \end{array} \tag{3}$$

The alteration leading from the first row of (3) to the second can be performed by n consecutive steps, replacing successively

$$\begin{array}{lll} a_{n-1} & \text{by} & a'_{n-1} = a_{n-1} + q\, a_n, \\ a_{n-2} & \text{by} & a'_{n-2} = a_{n-2} + q\, a'_{n-1}, \\ \cdots & \cdots & \cdots \\ a_0 & \text{by} & a'_0 \ = a_0 \ + q\, a'_1. \end{array} \tag{4'}$$

Since $q > 0$, the sign of a'_{n-1} can be different from the sign of a_{n-1} only when it is equal to the sign of a_n. Hence the first step of (4) either does not alter the sequence of the signs, or it generates an alteration of the first kind. Similarly for the other steps; thus if the sequence of the signs in the second row of (3) is different from the sequence of the signs in the first row, the alteration is composed of alterations of the first kind. The same statement holds for the alterations leading from any row of (3) to the following one. Hence the alteration leading from the coefficients of $f(x)$ to those of $\varphi(x - q)$ is composed of alterations of the first kind; conversely the alteration leading from φ to f is composed of alterations of the second kind.

Indeed if one interchanges f and ϕ and replaces q by $-q$, then the first row of (3) is transformed into the second one by equations

$$\begin{aligned} a'_{n-1} &= a_{n-1} - q\ a_n \\ &\cdots\cdots\cdots\cdots \\ a'_0 &= a_0 \quad - q\ a'_1. \end{aligned} \tag{4'}$$

Hence in this case, if the sign of a'_{n-1} differs from that of a_{n-1}, it must be opposite to the sign of a_n. From the corollaries of 5·221 it follows therefore: 1. The function $C(b)$ decreases when b increases. 2. When at any step in a Horner's scheme for a positive q, the first r coefficients are of the same sign, then the same holds for the final result of the scheme, and for expansions corresponding to all the higher values of b. 3. When at any step in a Horner's scheme for a negative q, the first r coefficients have alternating signs, then the same holds for the final result of the scheme and for the expansions corresponding to all the lower values of b. Suppose now that $a_n, \ldots, a_{n-r+1}$ have the same sign, say positive (without loss of generality) and $q > 0$, then it follows from (4) that

$$a'_{n-1} > a_{n-1}, \ \ldots, \ a'_{n-r+1} > a_{n-r+1},$$
$$a'_{n-r} = a_{n-r} + q\ a'_{n-r+1} \ > a_{n-r} + q\ a_{n-r+1}$$

for a suitable q, therefore $a'_{n-r} > 0$. Hence one can find a value of b for which the $r+1$ first signs are equal, and by repetition of the procedure one reaches a value of b such that all the signs are equal for this value of b and for all the higher values. For all these values of b, $C(b) = 0$. Suppose now that $a_n, \ldots, a_{n-r}$ have alternating signs and that $-q < 0$, then it follows from (4′) that

$$|a'_{n-1}| > |a_{n-1}|, \ \ldots, \ |a'_{n-r+1}| > |a_{n-r+1}|$$

and the signs are alternating. Let $a_{n-r+1} > 0$, then

$$a'_{n-r} = a_{n-r} - q\ a'_{n-r+1} < a_{n-r} - q\ a_{n-r+1}$$

is negative for a suitably chosen value of q. Similarly if $a_{n-r+1} < 0$, then a'_{n-r} can be made positive. Thus one can find a negative value $-q$ such that the first $r+1$ coefficients are alternating, and corresponding to the case of equal signs and positive q, one finds that there exists a value of b such that the signs are alternating for that value of b and all the smaller values. For all these values, $C(b) = n$. Hence

Theorem. $C(b)$ decreases steadily from n to 0 when b runs over the real axis.

5·223. *Budan-Fourier's theorem*. The function $C(b)$ has been proved by the last theorem to be a steadily decreasing function of the real variable b. As it takes integral values only, it is constant by segments; it changes its value at points of discontinuity only. At these points it decreases the saltus being an integral number. An alteration of $C(b)$ occurs where a coefficient of the polynomial changes its sign, and as these coefficients are continuous functions of b, a coefficient must take the value zero where it changes its sign. If an odd loss of changes occurs, the last sign is altered (see 5·221, lemma), *i.e.* the variable b passes through a root of the polynomial. The saltus of $C(b)$ at a root of $F(\xi)$ will now be investigated.

Let b be a root of $F(\xi)$, and let m be its multiplicity, m may be any positive integral number. Again, put $\xi - b = x$, and $F(\xi) = f(x)$. Then

$$f(0) = f'(0) = \ldots = f^{(m-1)}(0) = 0.$$

The coefficients of $f(x)$ are therefore

$$a_n, \ldots, a_m, 0, \ldots, 0, \text{ where } a_m \neq 0.$$

Apply Horner's scheme for a negative value $-q$; the second row will be

$$a_n, \ldots, a'_m, -q\,a'_m, \ldots, (-q)^m\,a'_m;$$

thus the second row has at least m changes more than the first row. a'_m is a continuous function of q; if therefore $|q|$ is small enough, a'_m has the same sign as a_m, and $(-q)^m\,a'_m = a'_0 = f(-q)$ has the same sign as a_m or a different sign, according as m is even or odd. The coefficients of $\phi(x) = f(x+q)$ show therefore $m + 2k$ more changes of sign than those of $f(x)$, where k is non-negative. By passing through an m-fold root of $F(\xi)$, the function $C(b)$ decreases by m or an even positive number more than m. In any interval (b,c) there exists a finite number (may be zero) of points of discontinuity of C; in the non-roots among them it changes by an even number, the alteration in any root is congruent (mod. 2) to the multiplicity of the root; hence the following theorem holds:

Theorem 1. Let $f(b) \neq 0$, $f(c) \neq 0$, $b < c$, and let r be the number of the roots of $f(x)$ in the interval (b, c), every root being counted with its own multiplicity, then

$$C(b) = C(c) + r + 2k,$$

where $k \geqq 0$ is an integral number.

Applying this theorem to an interval $(0, c)$, where c is chosen so great that $C(c) = 0$, one gets as a corollary

Descartes' rule. The number of the positive roots of $f(x)$ (every root being counted with its own multiplicity) is equal to the number of the changes of signs of the coefficients of $f(x)$ or to a number less than it by an even number.

The number of changes is not altered if one multiplies the coefficients of $f(x)$ with positive factors, e.g. if one replaces the coefficient of x^k by $f^{(k)}(b)$. Furthermore, one may write the sequence in the reverse order; in this case, the first element of the sequence may become zero, and the last element is constant; hence the elements equal to zero must be provided now with the sign of the next non-zero element on the *right* side. Using these notations, theorem 1 can be expressed as follows:

Budan-Fourier's theorem. Let $f(b) \neq 0$, $f(c) \neq 0$, then the number of the roots of $f(x)$ in the interval (b, c) (every root being counted with its own multiplicity) is equal to the difference of the numbers of changes of signs in the sets

$$f(b), f'(b), \ldots, f^{(n)}(b)$$

and

$$f(c), f'(c), \ldots, f^{(n)}(c),$$

or to a number less than it by an even number.

Put $x = \dfrac{cy + b}{y + 1}$ and therefore $y = \dfrac{x - b}{c - x}$, then the positive roots of $g(y) = (y + 1)^n f(x)$ are in $(1, 1)$—correspondence to the roots of $f(x)$ in the interval (b, c). Therefore the number of the roots in this interval can be found out by Descartes' rule.

These formulas do not always give directly the exact number of the roots in an interval, but they are very useful for getting it even in more complicated cases.

5·2231. *An example.* Consider again the example of 5·11.

$$f(x) = x^4 - 15x^3 + 68x^2 - 119x + 67.$$

As stated before, the real roots are positive and situated in the interval (1, 9). One could get this result also by considering the changes of signs. $f(-x)$ has no change and therefore no positive root, *i.e.* $f(x)$ has no negative root. From the previous calculations for this example one gets by considering the signs only:

$$C(0) = C(1) = 4$$
$$C(2) = 3$$
$$C(8) = 1.$$

Two roots have been computed already, one in the interval (1, 2), another in the interval (8, 9); to each of these roots, there corresponds a loss of one change. We want to find out, whether the loss of the two changes in (2, 8) corresponds to roots of $f(x)$. For this purpose, we try to approximate these suspected roots by Horner's scheme and get by very simple calculations

$$C(3) = 1 \qquad C(2.6) = 3$$

$$C(2.65) = 1 \qquad C(2.64) = 3.$$

Hence the two roots can only be situated in the interval $2.64 < x < 2.65$, but we shall prove that $f(x)$ is negative in this interval. As stated previously,

$$f(x) = 2 - 5(x-1) + 3(x-1)(x-2) + (x-1)(x-2)(x-3)(x-9)$$

$$= 2 - (x-1)\{5 - (x-2)[3 + (3-x)(9-x)]\}.$$

Hence for $2.64 < x < 2.65$, $f(x) < 2 - 1.64\{5 - 0.65[3 + 0.36.\ 6.36]\} < -0.6612$.

Hence $f(x)$ has only the two roots calculated in 5·12 and 5·14. The same result can also be obtained by calculating the discriminant and verifying that it is negative.

5·23. *Sturm's theorem.* By Budan-Fourier's theorem, the number of the roots in a given interval (b, c) is not determined uniquely, since the difference of the number of changes in the sequences

$$f(b),\ f'(b),\ \ldots,\ f^{(n)}(b) \tag{1}$$

and

$$f(c),\ f'(c),\ \ldots,\ f^{(n)}(c) \tag{1'}$$

may be greater than the number of the roots by an even number. Thus there arises the task of modifying the method used before by constructing a sequence of continuous functions

$$f_1(x),\ \ldots,\ f_m(x) \tag{2}$$

with the property that the number of changes $C'(b)$ in

$$f_1(b),\ \ldots,\ f_m(b) \tag{2'}$$

gives the exact number of the roots which are greater than b, or a number differing from it by a constant number only. Then

$$C'(b) - C'(c) \tag{3}$$

is equal to the number of the roots in the interval including its left (but not its right) endpoint. The solution of the problem is due to *J. K. Fr. Sturm*; it will be given in this article. Though Sturm's method is applicable to every case, it is not very convenient for practical calculation.

An m-fold root of $f(x)$ is an $(m-1)$-fold root of $f'(x)$ and therefore of the highest common factor $h(x) = (f(x), f'(x))$. Hence $f(x) : h(x)$ has the same roots as $f(x)$, each root being a simple one. As $f(x) : h(x)$ can be calculated by rational operations, one may replace $f(x)$ by $f(x) : h(x)$; thus there is no loss of generality in supposing that $f(x)$ has *simple roots only*. This supposition will be made now. The sequence (2) has to be arranged now in such a way that $C'(x)$ decreases by one in every root of $f(x)$, but is constant elsewhere.

Let $1<k<m$; if $f_k(x)$ changes its sign at $x=x_0$, and the sign of $f_{k-1}(x_0)$ is different from $f_{k+1}(x_0)$, then no change is gained or lost by $f_k(x)$ changing its sign. If however $f_{k-1}(x_0)$, $f_{k+1}(x_0)$ have the same sign, then two changes are either gained or lost. Now, the sequence (2) is proposed to be constructed in such a way that the number of the changes alters by one only, namely in the roots of $f(x)$, and decreases for increasing x. For this purpose a sequence will be constructed, where the number of changes is altered only when one of the outer elements changes its sign. Say $f_1(x)$ has the same sign as $f(x)$ and $f_m(x)$ has a constant sign. These considerations lead to the following theorem.

Sturm's theorem. Let (2) be a sequence of polynomials satisfying the following conditions:

1. $f_1(x)$ has the same sign as $f(x)$.
2. $f_2(x)$ .... $f'(x)$.
3. $f_m(x)$ has a constant sign.
4. if $1 < k < m$ and $f_k(x_0) = 0$, then $f_{k-1}(x_0)\, f_{k+1}(x_0) < 0$;

let $C'(x)$ be the number of the changes of sign in the sequence (2) for any particular value x, then the number of the roots of $f(x)$ in the interval (b, c) — the left endpoint b not being included — is given by (3).

Proof. The number of changes can be altered only by passing through those points which are roots of the polynomials forming the sequence. Let x_0 be such a point, and let $k = k_1, \ldots, k_s$ be the indices of the functions for which x_0 is a root. From 3 it follows that $k \neq m$. From 4 it follows that, for $1 < k < m$, the triplet of polynomials f_{k-1}, f_k, f_{k+1} contributes exactly one change in an interval containing x_0, but no other root of f_{k-1}, f_k or f_{k+1}. Thus $C'(x)$ is altered in the roots of $f_1(x)$ only, and its alteration is equal to the gain or loss of changes in the portion $f_1(x)$, $f_2(x)$ of the sequence (2). As there exist simple roots only, $f_1(x)$ changes its sign at any root x_0 of $f(x)$. If it changes from $-$ to $+$, $f(x)$ increases and therefore $f'(x) > 0$, and from 2 it follows that $f_2(x) > 0$; hence one change is lost. Similarly if $f(x)$ changes from $+$ to $-$, $f'(x)$ and therefore $f_2(x)$ is negative and one change is lost. Under the supposition made for the counting of the number of changes in 5·223, the zeros of $f_1(x_0)$ have to be counted with the sign of $f_2(x_0)$. Hence $C'(b) - C'(c)$ gives the number of the roots of $f(x)$ which are situated on the right of b but not on the right of c, that is in the interval $(b, c]$ which includes c and excludes b. Hence the theorem.

A sequence (2) satisfying the conditions of Sturm's theorem is called a *chain of Sturm*. It is possible to construct such a chain by the following rule

$$
\begin{aligned}
&f_1(x) = f(x)\\
&f_2(x) = f'(x)\\
-&f_3(x) = f_1(x) - q_2(x)\, f_2(x), \qquad 0 \leqq \text{degree } f_3(x) < \text{degree } f_2(x)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
-&f_{j+1}(x) = f_{j-1}(x) - q_j(x)\, f_j(x), \quad 0 \leqq \text{degree } f_{j+1}(x) < \text{degree } f_j(x)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}
$$

If n is the degree of $f(x)$, the procedure ends after not more than n steps; the last polynomial, say $f_m(x)$ is a common factor of the sequence; as $f_1(x) = f(x)$ and $f_2(x) = f'(x)$ have no common factor of positive degree, $f_m(x)$ is a positive or negative constant. Thus the conditions 1, 2 and 3 of Sturm's theorem are satisfied. Since $(f_{j-1}(x), f_j(x)) = f_m(x)$ is a constant, $f_{j-1}(x)$ and $f_j(x)$ have no common root. Let for $0 < k < m$, $f_k(x_0) = 0$, then $-f_{k+1}(x_0) = f_{k-1}(x_0) \neq 0$. Hence $f_{k+1}(x_0)\, f_{k-1}(x_0) = -f_{k-1}(x_0)^2 < 0$. Thus the sequence which is determined by (5) is a chain of Sturm. Other chains can be obtained, e.g. by multiplying the polynomials with arbitrary positive constants.

5·231*. *Legendre's polynomials.* Sturm's theorem will now be applied to *Legendre's polynomials*. Put

$$P_m(x) = \frac{1}{2^m \cdot m\,!}\, D^m[(x^2 - 1)^m], \quad m = 0, 1, 2, \ldots; \tag{1}$$

---

* May be omitted at a first reading.

D^m denotes the m^{th} derivate of the function written in [ ], and D^0 is this function itself. If u and v are polynomials in x,

$$D^m(u\,v) = \sum_{0}^{m} \binom{m}{s} D^{m-s}(u) D^s(v). \tag{2}$$

$$D^m[(x^2-1)^m] = D^{m-1}\,D[(x^2-1)^m] = D^{m-1}[(x^2-1)^{m-1}\,2mx],$$

whence from (2) it follows for $m > 1$

$$D^m[(x^2-1)^m] = 2mxD^{m-1}[(x^2-1)^{m-1}] + 2m(m-1)D^{m-2}[(x^2-1)^{m-1}]. \tag{3}$$

On the other hand, one gets from (2) for $m > 1$

$$2D^m[(x^2-1)^m] = 2D^m[(x^2-1)^{m-1}(x^2-1)] = 2(x^2-1)D^m[x^2-1)^{m-1}]$$
$$+ 4mxD^{m-1}[(x^2-1)^{m-1}] + 2m(m-1)D^{m-2}[(x^2-1)^{m-1}]. \tag{4}$$

By subtracting (3) from (4) and applying (1) , one gets

$$mP_m(x) = (x^2-1)\;P'_{m-1}(x) + mxP_{m-1}(x). \tag{5}$$

$$P_1(x) = x, \qquad P_0(x) = 1, \qquad P'_0(x) = 0,$$

(5) holds also for $m = 1$, and therefore generally.

From

$$D^{m+1}[(x^2-1)^m] = D^m[2mx(x^2-1)^{m-1}]$$
$$= 2mxD^m[(x-1)^{m-1}] + 2m^2\;D^{m-1}[(x^2-1)^{m-1}]$$

follows

$$P'_m(x) = xP'_{m-1}(x) + mP_{m-1}(x). \tag{6}$$

From (5) and (6) eliminate P'_{m-1}, and obtain

$$(x^2-1)\;P'_m(x) = mx\;P_m(x) - m\;P_{m-1}(x). \tag{7}$$

After replacing m by $m+1$ in (5), one gets

$$(m+1)\;P_{m+1}(x) = (x^2-1)\;P'_m(x) + (m+1)xP_m(x). \tag{5'}$$

From (7) and (5') eliminate $P'_m(x)$, then

$$(m+1)P_{m+1}(x) = (2m+1)xP_m(x) - mP_{m-1}(x). \tag{8}$$

Consider the sequence

$$P_n(x),\; P_{n-1}(x),\; \ldots,\; P_1(x),\; P_0(x) = 1 \tag{9}$$

in the interval

$$-1 \leqq x \leqq +1.$$

From (7) it follows for $m = n$, that if $P_n(x) = 0$, $P'_n(x)$ has the same sign as $P_{n-1}(x)$. If $P_{m-1}(x)$ and $P_m(x)$ have a common root, this root must also be a root of $P_{m-2}(x)$ as is seen from (8), and therefore of all subsequent polynomials of (9), in contradiction to $P_0(x) = 1$. Hence for $P_m(x) = 0$, $P_{m-1}(x) \neq 0$, and therefore it follows from (8) that $P_{m+1}(x)\ P_{m-1}(x) < 0$ at every root of $P'_m(x)$.

As $P_n(x)$ and $P_{n-1}(x)$ have no common root, it follows from (7) that $P_n(x)$ has no common root with its derivative and has therefore simple roots only. Hence (9) is a chain of Sturm in the interval $-1 \leqq x \leqq +1$ for every n.

From (7) it follows that

$$P_m(1) = P_{m-1}(1)$$

and

$$P_m(-1) = -P_{m-1}(-1).$$

As $P_0(x) = 1$, it follows that

$$P_m(1) = 1$$

and

$$P_m(-1) = (-1)^m.$$

The number of changes of sign in (9) is therefore $C'(-1) = n$, $C'(1) = 0$. Hence $P_n(x)$ has n different roots in the interval $(-1, 1)$. From (1) it follows that $P_n(x)$ is of degree n. Hence the roots of Legendre's polynomials are all situated in the interval $(-1, +1)$ and are simple roots.

5·24. *Method for calculation of roots.* To find out the roots of a polynomial, say

$$f(x) = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \tag{1}$$

one can proceed in the following manner : at first one has to determine an interval in which all the roots are situated. For this, put

$$t = 1 + |a_{n-1}| + \dots + |a_1| + |a_0|, \tag{2}$$

and suppose $x \geqq t$, then

$$x^n \geqq t\ x^{n-1} > |a_{n-1}|x^{n-1} + \dots + |a_1|\ x + |a_0|,$$

and therefore

$$0 < x^n - |a_{n-1}|x^{n-1} - \dots - |a_1|x - |a_0| \leqq f(x).$$

Hence for $x \geqq t$, $f(x) > 0$. Similarly for $(-1)^n f(-x)$:

for $x \leqq -t$, $f(x) < 0$, when n is odd

and $f(x) > 0$, when n is even.

At any rate, if there exists any real root of $f(x)$, it lies between $-t$ and $+t$. In general, it is not difficult to find out a smaller interval (a, b) in which all the roots of $f(x)$ are situated ; it suffices that the coefficients of the Taylor expansion of $f(x)$ for $x = a$ have alternating signs, whereas the coefficients of the Taylor expansion for $x = b$ are all positive. In this case $C(a) = n$, and $C(b) = 0$; therefore there cannot be any alteration of the monotone decreasing function C outside the interval (a, b).

If an interval containing all the roots has been determined, one subdivides the interval into smaller intervals. By Sturm's theorem one is able to decide how many roots are contained in each of these intervals ; the intervals containing roots are subdivided again, and the method is repeated. Given a positive number ϵ, to every root ξ of $f(x)$, there will be found out an interval of length $< \epsilon$, after a finite number of steps, such that ξ is situated in that interval. I.e. every root ξ is determined up to an *error* $< \epsilon$.

Though this method is absolutely sound in theory, a clever computor will hardly use it without essential modifications. The application of Sturm's method needs plenty of calculation, and one tries therefore to avoid it. It is mostly not difficult to get an idea about the general behaviour of the function $f(x) = y$ and the intervals where roots might be situated. For this purpose, graphical methods are very helpful (e.g. Lill's rectangular method *), provided the computor is sufficiently familiar with the theory and the practice of mathematical drawing. The method explained here aims to "separate" the roots, *i.e.* to find out intervals containing one root each, and to narrow each interval till its length does not exceed the admissible error. It is convenient to fix the error in advance ; this is done mostly by asking that a certain number of decimals must be correct. At every step of the calculation, one may neglect some digits, but one has to take care that the accumulated error must not influence the digits of the final result which are required. In this book, only the methods of the calculation can be explained, a skilful handling of them must be learnt by practice.

---

* See e. g. Bieberbach-Bauer, Vorlesungen über Algebra p.p. 134—140.

5·241. *Linear interpolation.* If $f(a)$ and $f(b)$ have different signs, the graph of the function $f(x)$ may be replaced by the straight line connecting the points with abscissae a and b. This line intersects the x-axis in $x = [af(b) - bf(a)] : [f(b) - f(a)]$. This value may be considered as a first approximation of the root. Consider the example of 5·1.

Put

$$x - 1 = y. \quad f(x) = g(y) = y^4 - 11y^3 + 29y^2 - 24y + 2$$

$$g(0) = 2, \; g(1) = -3.$$

The approximation by the straight line leads to $y = 0.4$ which is obviously too great. Of course the graph of the polynomial in that interval is very different from a straight line. Now

$$\begin{array}{ll} g(0) = 2 & g(1) = -3 \\ g'(0) = -24 & g'(1) = 5. \end{array}$$

The graph is therefore considerably bent in the interval, and the root must lie near the point $x - 1 = 0$. For the suitability of the approximation by linear interpolation, it is essential that the derivate does not change its sign in the interval.

5·242. *Newton's method.* The graph of $y = f(x)$ can be approximated by its tangent for an interval near the point of contact. This means that in the Taylor expansion of the polynomial at the point of contact, the terms which are of the second and of higher degree are omitted. When the interval is small, and the coefficient of the linear term is small in comparison to the coefficients of the higher terms, this approximation furnishes good results. Applied to the previous example, Newton's method furnishes $y = 1 : 12$. This approximation was indeed the starting point for the calculation of the same example by Horner's method in 5·12.

If an approximation of a root is obtained which is already near to the root, then Horner's method furnishes a Taylor expansion for this approximation :

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

in which, for small values of x, the higher terms are of a small influence (unless a_1 is small in comparison with the coefficients of the higher terms). Let x_1 be an approximation of a root of $f(x)$ which lies near to 0, and put

$$x_2 = -[a_n x_1^n + \ldots + a_2 x_1^2 + a_0] : a_1,$$

then x_2 is in general a better approximation of that root. By applying this method to the example considered just before, and putting $x_1 = 1 : 12$, one gets $x_2 = 0.091 \dots$ which is a little too small. Indeed the value of the roots has been stated in 5·12 to be equal to $0.0935324 \dots$.

The methods explained here are very helpful if applied in connection with Horner's scheme, especially when single roots are required. When all the roots are asked for, it is often better to apply Graeffe's method which will be explained in 5·3.

5·25. *Poulain's theorem.*

The number of the real roots of a polynomial with real coefficients is interconnected with the corresponding number of a different polynomial by a theorem named after Poulain.

Poulain's theorem. Let $h(z) = b_m z^m + \dots + b_1 z + b_0$ be a polynomial with real coefficients and real roots only, let $b_m \neq 0$, $b_0 \neq 0$, and let $f(x)$ be a polynomial with real coefficients, then the number of the different real roots of

$$g(x) = b_0\, f(x) + b_1\, f'(x) + \dots + b_m\, f^{(m)}\,(x)$$

is not less than that of $f(x)$, and the corresponding proposition holds, when each root has been counted with its own multiplicity.

This theorem is a generalisation of the following lemma.

Lemma. Let $a \neq 0$, then the number of different real roots of $af(x) + f'(x)$ is not less than the number of different real roots of $f(x)$, and the corresponding proposition holds, when each root has been counted with its multiplicity.

Proof of the lemma. Let m_1 be the number of the different real roots of $f(x)$, and let m_2 be the number of its real roots when each root is counted with its own multiplicity; also let m'_1 and m'_2 denote the corresponding numbers for $k(x) = af(x) + f'(x)$. The proof will be given in several steps. At first it will be proved that

$$m'_1 \geqq m_1 - 1 \tag{1}$$

and that

$$m'_2 \geqq m_2 - 1, \tag{2}$$

then it will be shown :

$$m'_1 \neq m_1 - 1 \tag{3}$$

and
$$m'_2 \neq m_2 - 1. \tag{4}$$

This will prove the lemma.

(1) Let $c_1, c_2, \ldots, c_{m_1}$ be the different real roots of $f(x)$ written in ascending order, forming $m_1 - 1$ consecutive intervals. It will be proved that $k(x)$ changes its sign in each of these intervals. The sign of $f(x)$ in anyone of these intervals is constant; suppose (without loss of generality) it to be positive in (c_1, c_2). Hence $f(x)$ increases in a sub-interval (c_1, c') and decreases in (c'', c_2). If r_1 is the multiplicity of the root c_1 of $f(x)$, then $f'(x)$ has a root of multiplicity $r_1 - 1$ in c_1. Since the number of roots of $f'(x)$ is finite, one can suppose that $f'(x)$ has no root inside the interval (c_1, c'), it is therefore positive in the interval and is either positive or zero at c_1, according as $r_1 = 1$ or $r_1 > 1$. In the first case, it is obvious that $k(x)$ has the same sign as $f'(x)$ in a sub-interval (c_1, d') of (c_1, c'), where $c_1 < d' < c'$, and d' is suitably chosen, but even if $r_1 > 1$, the quotient $af(x) : f'(x)$ tends to 0 if x tends to c_1, and therefore $k(x)$ has the same sign as $f'(x)$ in a suitably chosen interval (c, d'). Thus $k(x)$ is positive in (c_1, d'), and in the same manner it is shown that $k(x)$-is negative in an interval (d'', c_2). Hence $k(x)$ changes its sign in (c_1, c_2), and there exists therefore a root of $k(x)$ in this interval. Correspondingly for each of the $m_1 - 1$ intervals. Hence (1) holds.

(2). If $f(x)$ has a root of multiplicity r_i in c_i (for $i = 1, \ldots, m_1$), then $f'(x)$ has a root of multiplicity $r_i - 1$, and $k(x) = af(x) + f'(x)$ has also a root of multiplicity $r_i - 1$ in c_i, where a root of multiplicity 0 means that there is no root at that point. By counting the roots of $k(x)$ in $c_1, \ldots, c_{m_1}$ with their multiplicity and considering that in every interval (c_i, c_{i+1}) at least one root of $k(x)$ is situated, one gets the inequality

$$m'_2 \geqq \sum_{1}^{m_1} (r_i - 1) + (m_1 - 1) = \Sigma r_i - 1 = m_2 - 1.$$

Hence (2) is proved.

(3 and 4). $f(x)$ and $k(x)$ are of the same degree, say n. As the number of the complex roots is even, $m_2 \equiv n \equiv m'_2 \pmod{2}$. This rules out $m'_2 = m_2 - 1$; hence (4) holds. Suppose now $m'_1 = m_1 - 1$. As $k(x)$ changes its sign in each interval (c_i, c_{i+1}), it has exactly one root in each of these intervals; this root is of odd multiplicity and $k(x)$ has no other roots. Hence $c_1, \ldots, c_{m_1}$ are non-roots of $k(x)$ and therefore simple roots of $f(x)$. From these considerations it follows that

$$m_1 = m_2 \equiv n \pmod{2}.$$

But, as the roots of $k(x)$ are of odd order, $m'_1 \equiv m'_2 \pmod{2}$. Hence $m_1 - 1 \equiv m'_2 \equiv n \pmod{2}$, and this consequence contradicts $m_1 \equiv n \pmod{2}$. Hence the supposition $m'_1 = m_1 - 1$ leads to a contradiction, and therefore (3) holds. As (1), (2), (3), (4) are proved, the lemma holds.

Proof of Poulain's theorem.

Without any loss of generality suppose that $b_m = 1$. Hence for $m = 1$, $g(x) = b_0 f(x) + f'(x)$, and in this case the theorem is reduced to the lemma. Let $p > 0$, and suppose the theorem holds for $m = p$. We shall prove it for $m = p + 1$. If a is a root of $h(z)$, then $a \neq 0$, and $h(z) = (z - a)\, h_1(z)$, where $h_1(z)$ has real roots only.

Let $h_1(z) = z^p + \ldots + c_1\, z + c_0$. As the theorem holds for $m = p$, the number of the roots of $g_1(x) = \sum\limits_0^p c_i\, f^{(i)}(x)$ is greater than or equal to the number of the roots of $f(x)$. In this formula $f^{(0)}(x)$ means $f(x)$.

$$g'_1(x) = \sum_0^p c_i\, f^{(i+1)}(x).$$

If one replaces the powers of z in $h(z) = (z - a)\, h_1(z)$ by the corresponding derivates of $f(x)$, one gets

$$g(x) = g'_1(x) - a\, g_1(x).$$

From the preceding lemma it follows that the number of the roots of $g(x)$ is not smaller than the number of the roots of $g_1(x)$, and therefore not smaller than the number of the roots of $f(x)$. Hence the theorem holds.

5·3. *Graeffe's Method.*

By Graeffe's method all the roots of a polynomial are calculated simultaneously without any previous separation of them or any other preparatory measure. The method leads very quickly to useful results when the roots are different and real It is often difficult to estimate the error made in neglecting higher decimals ; thus one should check the results afterwards.

5·31. *Real distinct roots.* Let $b_1, b_2, \ldots, b_n$ be the roots of the polynomial $a_0 x^n + a_1 x^{n-1} + \ldots + a_n$, and let

$$|b_1| > |b_2| > \ldots > |b_n|, \tag{1}$$

then

$$-\frac{a_1}{a_0} = b_1\left(1 + \frac{b_2}{b_1} + \ldots + \frac{b_n}{b_1}\right) = b_1(1 + \varepsilon_1)$$

$$-\frac{a_2}{a_1} = -\frac{a_2}{a_0} : \frac{a_1}{a_0}$$

$$= \frac{b_1\, b_2\left(1 + \frac{b_3}{b_1} + \ldots + \frac{b_n}{b_1} + \frac{b_3}{b_2} + \ldots + \frac{b_n}{b_2} + \frac{b_3\, b_4}{b_1\, b_2} + \ldots + \frac{b_{n-1}\, b_n}{b_1\, b_2}\right)}{b_1(1 + \varepsilon_1)}$$

$$= b_2(1 + \varepsilon_2)$$

…………………………………………………………………………

$$-\frac{a_{n-1}}{a_{n-2}} = b_{n-1}(1 + \varepsilon_{n-1})$$

$$-\frac{a_n}{a_{n-1}} = (-1)^n \frac{a_n}{a_0} : \left(\frac{-a_1}{a_0}\; \frac{-a_2}{a_1} \;\ldots \frac{-a_{n-1}}{a_{n-2}}\right)$$

$$= \frac{b_1 \ldots b_n}{b_1(1 + \varepsilon_1) \ldots b_{n-1}(1 + \varepsilon_{n-1})} = b_n(1 + \varepsilon_n).$$

If $|b_i : b_{i+1}|$ is very great, for $i = 1, \ldots, n$, the numbers ε_i can be omitted. In this case, one gets the approximation

$$b_i \sim -\frac{a_i}{a_{i-1}}, \text{ for } i = 1, \ldots, n. \tag{2}$$

In general (2) is not a consequence of (1), but for a suitable exponent m the quotients $b_{i+1}{}^m : b_i{}^m$ become negligible. Therefore, one has to find out a polynomial, whose roots are $b_1{}^m, \ldots, b_n{}^m$. The coefficients of this polynomial are symmetric functions of $b_1, \ldots, b_n$, hence it is possible to calculate them as rational functions of $a_0, a_1, \ldots, a_n$ with rational coefficients. The calculation for an arbitrary m is tiresome, but it is easy to find out a polynomial whose roots are the squares of the roots of $f(x)$, and by repeating this construction one gets polynomials with the roots

$$b_1{}^2,\ b_1{}^4,\ b_1{}^8, \ldots, b_1{}^{2^k} \ldots.$$

Let $a'_0 x^n + a'_1 x^{n-1} + \ldots + a'_n$, $a'_0 = a_0{}^m$ have the roots $b_1{}^m, \ldots, b_n{}^m$, and let m be chosen so great that $b_{i+1}{}^m : b_i{}^m$ may be neglected, then

$$b_i{}^m \sim -\frac{a'_i}{a'_{i-1}} \text{ holds.}$$

The corresponding holds for the polynomial with the roots $b_1{}^{2m}, \ldots, b_n{}^{2m}$; hence the absolute values of its coefficients become approximately the squares of the corresponding coefficients a'_i. Hence one has to repeat the construction of polynomials till the calculation shows that after further repetition, the coefficients will be practically the squares of the coefficients of the preceding polynomial. To get a polynomial whose roots are the squares of the roots of $f(x)$, calculate

$$\begin{aligned}(-1)^n f(x)\, f(-x) &= a_0(x-b_1)\ldots(x-b_n)\; a_0(x+b_1)\ldots(x+b_n)\\ &= a_0^2(x^2-b_1^2)\ldots(x^2-b_n^2)\\ &= f_2(x^2).\end{aligned}$$

The coefficients of f_2 will be calculated by the following scheme

$$\begin{array}{llllll} (1) & a_0 & a_1 & a_2 & \ldots & a_n \\ & a_0 & -a_1 & a_2 & & \pm a_n \\ \hline (2) & a_0^2 & -a_1^2 & a_2^2 & \ldots & \pm a_n^2 \\ & & +2a_0\, a_2 & -2a_1\, a_3 & & \\ & & & +2a_0\, a_4 & & \end{array}$$

As in the first pair of lines corresponding numbers differ only by the sign, one uses to write only the signs in the second line. The numbers increase very quickly; therefore it is convenient to omit the last figures, simultaneously denoting the decimals very clearly. For this purpose replace the decimal point by an index which is equal to the exponent of the power of 10 with which the decimal fraction is to be multiplied. E.g.

$$3^{n}456131 \qquad \text{for} \qquad 3{\cdot}456131\ 10^{n}.$$

To extract the roots at the end of the calculation, we need logarithms. It is therefore useless to calculate more decimals than the tables of logarithms contain.

Example. $x^3 - 10x^2 + 16x - 2 = 0$

$$\begin{array}{lllll} (1) & 1 & -1^{1}0 & 1^{1}6 & -2 \\ & + & + & + & + \\ \hline & 1 & -1^{2}0 & 2^{2}56 & -4 \\ & & +0\ 32 & -0\ 4 & \\ \hline (2) & 1 & -6^{1}8 & 2^{2}16 & -4 \\ & + & + & + & + \\ \hline & 1 & -4^{3}624 & 4^{4}6656 & -16 \\ & & +0\ 432 & -0\ 0544 & \end{array}$$

(4)	1	$-4^{3}1802$	$4^{4}6112$	-16
	$+$	$+$	$+$	$+$
	1	$-1^{7}75729$	$2^{9}12631$	-256
		$+0\ 00932$	$-0\ 00013$	
(8)	1	$-1^{7}74797$	$2^{9}12618$	-256

At the next step the coefficients will be the squares of the preceding coefficients, and in no case the error will have influence on the first 5 figures. Therefore stop the procedure, and calculate now the roots by the help of logarithms.

log. of |coeffs.|	log. x^8	log. $\|x\|$	$\|x\|$
0	7.24254	0.90532	8.0412
7.24254	2.08506	0.26063	1.8223
9.32760	1.08064—8	0.13508 − 1	0.1365
2.40224			
		0.30103	10.0000
		= log 2	

The sign of the roots cannot be determined by Graeffe's method ; one must make a special investigation for the sign in every case. In this example the coefficients have alternating signs, hence the roots are all positive. *Verification* : form the elementary symmetric functions of the approximate roots and compare :

$$s_1 = 10, \qquad s_2 = 15.9998 \qquad s_3 = 2$$

for 10 16 2.

5-32. *Complex roots.* If a real polynomial has complex roots, two of them are always conjugate, and these have therefore the same absolute value. Thus Graeffe's method has to be modified in this case. An example will give valuable hints for necessary modifications.

Example.

$$x^4 - 11x^3 + 29x - 24x + 2$$

This polynomial has already been considered in § 1, and it is known to have two real and two complex roots. Apply now the scheme* of Graeffe's method

	1	− 11	29	− 24	2
(1)	1	− 121	841	− 576	4
		58	− 528	+ 116	
			+ 4		
(2)	1	− 63	317	− 460	4
	1	−3969	100489	−211600	16
		+ 634	− 57960	+ 2536	
			8		
(4)	1	− 3335	42537	−209064	16
	1	$-1^{7}11222$	$1^{9}80938$	$-4^{10}3707$	256
		+ 851	−1 41525	0	
			0		
(8)	1	$-1^{7}10371$	$3^{8}9413$	$-4^{10}3707$	256

If the procedure is repeated, the two first and the two last coefficients will become the squares of the corresponding coefficients of the line (8), but the third coefficient will depend also upon the second and the fourth. We cannot expect that further repetition of the procedure will make the third coefficient independent of its neighbours, as two roots of the polynomial have an equal absolute value. If b_1 is greater than the absolute value of the complex roots, then

$$-\frac{a'_1}{a'_0}=b_1^m\left(1+\frac{b_2^m+b_3^m+b_4^m}{b_1^m}\right)\sim b_1^m, \text{ for a suitable } m.$$

A rough mental calculation shows that $b_1^2 \sim 60$, $b_1^8 \sim 1^{7}2$.

The same consideration for $f(\frac{1}{x})$ shows that, if $b_4^m < |b_2|^m, -\frac{a'_4}{a'_3} \sim b_4^m$ holds. Hence the complex roots are only dependent on the 3 middle coefficients. In order to get the law of dependence, the considerations will now be generalised.

---

* As the signs in the second line are all +, we omit these lines for abbreviation.

Let B and C be two intervals, so that every number of C is very small in comparison to the numbers of B, and let

$$f(x) = a_0\, x^n + \ldots + a_{n-1}\, x + a_n$$

have two sets of roots:

$b_1, b_2, \ldots, b_r$ whose absolute values belong to B, and

$c_1, c_2, \ldots, c_s$ whose absolute values belong to C, where $r + s = n$.

Let y be a number of B, and d a number of C; represent the coefficients of $f(x)$ by its roots and approximate these by y and d respectively. As d is small in comparison to y,

$a_k \sim (-1)^k \binom{r}{k} a_0\, y^k$, for $k \leqq r$, and $a_m \sim (-1)^m \binom{r}{m} a_0\, y^r\, d^{m-r}$ for $m \leqq r$.

Hence

$$\begin{aligned} \frac{f(y)}{y^s} &= a_0\, y^r + \ldots + a_r + a_{r+1}\, y^{-1} + \ldots + a_r\, y^{-s} \\ &\sim a_0\, y^r + \ldots + a_r = f_1(y). \end{aligned}$$

Let y be one of the roots b_i, then $f_1(y) \sim 0$. Hence the roots b_i can be approximated by the roots of $f_1(x)$.

Let $x = 1 : z$, then $a_n\, z^n + \ldots + a_1\, z + a_0$ has the roots

$$\frac{1}{c_1} = b'_1, \ldots, \frac{1}{c_s} = b'_s, \text{ and } \frac{1}{b_1} = c'_1, \ldots, \frac{1}{b_r} = c'_r;$$

the absolute values of b'_i belong to an interval B′, the absolute values of c'_k belong to C′, and every number of C′ is small in comparison to those of B′. Hence the roots b'_i can be approximated by the roots of $a_n\, z^s + \ldots + a_r$, and therefore the roots c_i of $f(x)$ can be approximated by the roots of

$$a_r\, x^s + a_{r+1}\, x^{s-1} + \ldots + a_n.$$

Thus the polynomial $f(x)$ has to be split into two polynomials, the first is defined by the $r + 1$ upper terms and leads to the upper class of roots; the second one is defined by the $s + 1$ lower terms and leads to the lower class of roots. The two classes may also be divided into sub-classes etc. Finally we get classes

$$b_{1,1}, \ldots, b_{1,r_1};\; b_{2,1}, \ldots, b_{2,r_2};\; \ldots;\; b_{k,1}, \ldots, b_{k,r_k},$$

each root being small in comparison with the roots of the preceding classes, and to each class corresponds a polynomial, which can be cut out from $f(x)$. The ratio of the absolute value of the roots increases when we replace these roots by higher powers of them, therefore we get finally by Graeffe's method k polynomials each of them having only roots with the same absolute value. In the previous example these polynomials are

$$x - 1^{7}10371, \quad 1^{7}10371\, x^2 - 3^{8}9413\, x + 4^{10}3707, \quad 4^{10}3707\, x - 256.$$

From these polynomials one gets the roots of $f(x)$:

$$8 \log |b_1| = 7.04286 \qquad \log |b_1| = 0.88036 \qquad |b_1| = 7.592$$

$$8 \log |b_4| = 7.76769 - 16 \qquad \log |b_4| = 0.97096 - 2 \qquad |b_4| = 0.093532$$

$$16 \log |b_2| = \log 4^{10}3707 - \log 1^{7}10371$$

$$= 3.59767 \qquad \log |b_2| = 0.22476 \qquad |b_2| = 1.6779$$

$$\log \cos 8\phi = \log 3^{8}9413 - 8 \log |b_2| - \log 2 - \log 1^{7}10371 = 9.35293 - 10$$

$$8\phi = + 73^\circ 31' \quad + k360^\circ$$

$$\phi = \pm 9^\circ 11' 23'' + k45^\circ.$$

To finish this calculation, one must fix the signs of the real roots and determine the integral number k. As the signs of the coefficients are alternating, there is no negative root. Hence $b_1 = 7.592\ldots$, $b_4 = 0.093532\ldots$ These numbers correspond to the results obtained in 5·1 by Horner's method and by Lagrange's method.

As $b_1 + b_2 + b_3 + b_4 = 11$, $2r \cos \phi = 3.315 \ldots$. But as $2r = 3.356 \ldots$, ϕ must be a very small angle. Hence $k = 0$.

$$b_2 = 1.6567 + i\, 0.26803$$

$$b_3 = 1.6567 - i\, 0.26803.$$

Verification: $\log b_1 + \log b_4 + 2 \log r = 0.30104$

for $\log 2 = 0.30103$

$b_1 + b_2 + b_3 + b_4 = 10.999$

for $11.$

The result can be corrected by further calculation. As seen from the results of 5·1 and from the checking given here, b_1, b_4 and r are very exact. The correction is therefore expected to concern mainly the angle ϕ, whose true value may be a little smaller. As ϕ itself is a small angle, this correction will materially affect $\sin \phi$. Hence the imaginary parts of b_2 and b_3 are true up to the second decimal only.

If a polynomial with roots of equal absolute value has a degree > 2, either it has multiple roots, or it has non-conjugate roots with the same absolute value. The multiple roots can be removed by division by the h. c. f. of the polynomial and its derivative. Non-conjugate roots of equal absolute value can be cleared away by Horner's scheme, *viz.*, if $|x| = |x'|$ and x' is different from $\bar{x}$ and x, then $|x - a| \neq |x' - a|$.

Hence the real and the complex roots of $f(x)$ can be found out in every case by a combination of Graeffe's method and Horner's scheme. The results should be verified and it is possible to minimise the error by the methods given in 5-1.

5-4. *Roots of complex polynomials.*

Let $\phi(x)$ be a polynomial with complex coefficients,

$$\phi(x) = x^n + a_{n-1}\, x^{n-1} + \ldots + a_1\, x + a_0$$

$$\bar{\phi}(x) = x^n + \bar{a}_{n-1}\, x^{n-1} + \ldots + \bar{a}_1\, x + \bar{a}_0$$

$$(\phi(x), \overline{\phi}\,(x)) = f_1(x),\ \phi(x) = f_1(x)\ \phi_1(x),\ \overline{\phi(x)} = f_1(x)\ \bar{\phi_1}(x)$$

$$\phi_1(x)\ \overline{\phi_1(x)} = f_2(x),$$

then $f_1(x)$ and $f_2(x)$ are real polynomials, and every root of $\phi(x)$ is either a root of $f_1(x)$ or of $f_2(x)$. Of two conjugate roots of $f_2(x)$, one only is a root of $\phi(x)$, the other one is a root of $\bar{\phi}(x)$. Thus by applying Graeffe's method to $f_1(x)$ and to $f_2(x)$, and eventually verifying, it is always possible to find out the roots of $\phi(x)$.

5-41. *Circles enclosing the roots of $\phi(x)$.* As in 5-24, put

$$t = 1 + |a_{n-1}| + \ldots + |a_1| + |a_0|.$$

It will be shown that the roots of $\phi(x)$ are situated inside a circle of radius t about the origin. For this, it is necessary and sufficient to prove that $|\phi(x)|$ is positive for $|x| \geqq t$. The proof is nearly the same as in 5-24.

$$|x|^n > t|x|^{n-1} \geqq |a_{n-1}|\,|x|^{n-1} + \ldots + |a_1|\,|x| + |a_0| \geqq |a_{n-1}\, x^{n-1} + \ldots + a_0|;$$

hence $$0 < |x^n| - |a_{n-1}\, x^{n-1} + \ldots + a| \leqq |\phi(x)|.$$

By the following consideration, it is often possible to find out a smaller circular domain with a centre different from the origin such that all the roots of $\varphi(x)$ are contained in it. Without loss of generality, one may suppose that the coefficients of $\varphi(x)$ are all real (as every root of $\varphi(x)$ is a root of $f_1(x)\,f_2(x)$). By a suitable transformation, $x = x' + a$, one obtains a polynomial $f(x') = \varphi(x)$ with positive coefficients only. To a circular domain $|x'| \leqq b$, there corresponds a circular domain in the x-plane which has the centre a and the radius b. Thus one can apply the following generalisation of Kakeya's theorem to find out that the roots of $\varphi(x)$ are situated between two concentric circles.

Theorem. Let the coefficients of $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be positive and $0 < p < \frac{a_{k-1}}{a_k} < q$, for $k = 1, \ldots, n$, then the roots of $f(x)$ satisfy the condition

$$p < |x| < q.$$

Proof. Let $x = q\,y$, $f(x) = g(y) = \Sigma\, b_k\, y^k$, then $b_k = q^k\, a_k$. Hence $b_{k-1} : b_k < 1$. From Kakeya's theorem it follows therefore for the roots that $|y| < 1$, and $|x| < q$. The roots of $F(z) = a_0\, z^n + \ldots + a_{n-1}\, z + a_n$ are reciprocal to the roots of $f(x)$. As $\frac{a_{n-k+1}}{a_{n-k}} < \frac{1}{p}$ holds, it follows from the first part of the proof that the roots of F must satisfy $|z| < \frac{1}{p}$. Hence $|x| = |\frac{1}{z}| > p$ for the roots of $f(x)$, and therefore the theorem holds.

5·42. *Interconnection between the roots of a polynomial and those of its derivative.*

Theorem of Gauss. Every convex polygon enclosing all the roots of $\varphi(x)$ contains every root of $\varphi'(x)$.

Proof. Let γ be an arbitrary root of φ' and $\beta_1, \ldots, \beta_n$ be the roots of φ. Without any loss of generality, one may suppose that γ is not a root of φ. Then

$$\frac{\varphi'(x)}{\varphi(x)} = \sum \frac{1}{x - \beta_i}; \text{ hence } 0 = \frac{\varphi'(\gamma)}{\varphi(\gamma)} = \sum \frac{1}{\gamma - \beta_i}.$$

and therefore

$$0 = \Sigma \frac{1}{\gamma - \beta_i} = \Sigma \frac{\gamma - \beta_i}{|\gamma - \beta_i|^2} = \Sigma(\gamma - \beta_i)b_i,$$

where every b_i is positive. In the complex plane, the numbers $\beta_i - \gamma$ represent vectors which start from γ and lead to $\beta_1, \ldots, \beta_n$. Project the vectors $b_i(\beta_i - \gamma)$ orthogonally on any straight line of the complex plane; then the sum of those "components" must be zero, as the sum of the vectors themselves is zero. Consider in particular two straight lines g_1 and g_2 intersecting in γ orthogonally. If all the points β_i are situated on the same side of g_1, then the components of $\beta_i - \gamma$ on g_2 have all the same sign, and the same holds for the components of $b_i(\beta_i - \gamma)$ as the numbers b_i are positive. This is impossible, as the sum of the components of those vectors along g_2 is equal to zero. Hence there exists no line g_1 passing through any root of $\phi'(x)$ such that the roots β_i of $\phi(x)$ lie all on the same side of g_1. Let now P be a convex polygon including all the roots of ϕ. If γ is outside of P, we can draw through γ a straight line g not intersecting P. Hence P, and therefore all the roots of ϕ, are situated on the same side of g. Hence γ is not a root of ϕ'. Hence the theorem.

Let P_0 be the smallest convex polygon including the roots of ϕ (the reader may prove that such a polygon exists and is unique.). P_1 the corresponding polygon defined by ϕ', ..., P_i the smallest polygon containing the roots of $\phi^{(i)}$. The polygons with higher indices are included in the preceding ones. $\phi^{(n)}$ degenerates to the point $\frac{1}{n} - \frac{a_{n-1}}{a_n} = \frac{1}{n} \Sigma\beta_k$. This point is the centre of gravity of the roots of ϕ, and for the same reason it is the centre of gravity of the roots of ϕ' and of the roots of each derivate.

5·5. *Interpolation.*

Let

$$\beta_1, \ldots, \beta_{n+1}$$

be n + 1 *different* elements of an arbitrary field K, and let

$$\lambda_1, \ldots, \lambda_{n+1}$$

be n + 1 arbitrary elements of K. Wanted a polynomial $f(x)$ of K[x] so that $f(\beta_i) = \lambda_i$ for i = 1, ..., n + 1, and degree $f(x) \leq$ n.

Let $f(x) = \alpha_0 + \dots + \alpha_n x^n$. This polynomial has the proposed properties if and only if its coefficients satisfy

$$\sum_0^n \alpha_i \beta_k^i = \lambda_k.$$

The determinant of this system of n + 1 linear equations (see 3-53) is equal to $\pm \prod_{i<j} (\beta_i - \beta_j)$ and is $\neq 0$, as the n + 1 elements β_i are supposed to be different. Hence the problem has one and only one solution. This solution can be calculated by the methods explained in Ch. I, but it is easier to get it from special cases.

5-51. *Lagrange's formula.* Let $f_k(x)$ be the solution if $\lambda_{i \neq k} = 0$, $\lambda_k = 1$, then $f(x) = \sum_1^{n+1} \lambda_k f_k(x)$ is the solution for arbitrary λ-elements.

But $f_k(x) = \dfrac{g(x)}{(x - \beta_k)\, g'(\beta_k)}$, where $g(x) = \prod_1^{n+1} (x - \beta_i)$, satisfies the above requirements. So we get *Lagrange's formula for interpolation*.

$$f(x) = \sum g(x) \frac{\lambda_k}{(x - \beta_k)\, g'(\beta_k)}.$$

5-52. *Interpolation by successive calculation.* By Lagrange's formula the problem of interpolation has been solved in the most complete and general manner, but the formula is not convenient for practical calculation. It is easier to calculate the coefficients of the product-representation of $f(x)$

$$f(x) = \gamma_0 + \gamma_1(x - \beta_1) + \gamma_2(x - \beta_1)(x - \beta_2) + \dots + \gamma_n(x - \beta_1) \dots (x - \beta_n),$$

where $\gamma_0 = f(\beta_1) = \lambda_1$, $\gamma_1 = \dfrac{\lambda_2 - \lambda_1}{\beta_2 - \beta_1}$, and one may calculate the coefficients γ_i successively. When K is the field of the real numbers, it is convenient to arrange the calculation in the following manner.

Let $f_i(x)$ be defined by $f_0(x) = f(x)$, and for $k = 1, \dots, n$,

$$f_k(x) = \frac{f_{k-1}(x) - f_{k-1}(\beta_k)}{x - \beta_k},$$

then $$f_i(x) = \gamma_i + \gamma_{i+1}(x - \beta_{i+1}) + \dots + \gamma_n(x - \beta_{i+1}) \dots (x - \beta_n). \qquad (1)$$

Hence $f_n(x) = \gamma_n$. Therefore calculate the values

$$\{k, m\} = f_k(\beta_m), \text{ for } k = 0, \dots, n, \quad k < m \leqq n + 1$$

by $\{k, m\} = [\{k-1, m\} - \{k-1, k\}] : (\beta_m - \beta_k)$

and $\{0, m\} = \lambda_m$. We calculate the values column-wise in the following scheme

$$\begin{array}{llllll}
 & \{0, m\} & \{1, m\} & \{2, m\} & \dots & \{n, m\} \\
\{k, 1\} & \lambda_1 & & & & \\
\{k, 2\} & \lambda_2 & \dfrac{\lambda_2 - \lambda_1}{\beta_2 - \beta_1} & & & \\
\{k, 3\} & \lambda_3 & \dfrac{\lambda_3 - \lambda_1}{\beta_3 - \beta_1} & \dfrac{\{1, 3\} - \{1, 2\}}{\beta_3 - \beta_2} & & \\
\cdot & \cdot & & & & \\
\cdot & \cdot & & & & \\
\cdot & \cdot & & & & \\
\{k, n+1\} & \lambda_{n+1} & \dfrac{\lambda_{n+1} - \lambda_1}{\beta_{n+1} - \beta_1} & \dfrac{\{1, n+1\} - \{1, 2\}}{\beta_{n+1} - \beta_2} & \dots & \dfrac{\{n-1, n+1\} - \{n-1, n\}}{\beta_{n+1} - \beta_n}
\end{array}$$

The first elements of the different columns of this scheme form the set $\gamma_0, \gamma_1, \dots, \gamma_n$ of the coefficients of (1). This scheme is easier for calculation than Lagrange's formula.

5·53. *Newton's formula.* The calculation can be further simplified if the elements $\beta_1, \dots, \beta_{n+1}$ are equidistant, *i.e.* if

$$\beta_{k+1} - \beta_k = \Delta$$

for every k; then

$$\Delta\{k, m\} = [\{k-1, m\} - \{k-1, k\}] : (m-k)$$

$$= \frac{1}{m-k} \sum_{i=k}^{m-1} \Delta_{k-1, i},$$

where $\Delta_{k-1, i} = \{k-1, i+1\} - \{k-1, i\}$ is the difference of two consecutive elements in the preceding column. So $\Delta\ \{k, m\}$ is the mean-value of the differences of consecutive elements of the rows m to k in the column $k-1$. Now in the cases under consideration, the scheme will be transformed in such a way that the differences of consecutive elements only will be calculated. For this purpose, the notations of the calculus of differences will be introduced here.

Let $\Delta_x u = x - \beta_1$, then $\Delta_x(u - k - 1) = x - \beta_k$.

Let
$$F(u) = f(x) = f(\Delta_x u + \beta_1) = \gamma_0 + \gamma_1 u\Delta_x + \gamma_2 u(u-1)\Delta_x^2 + \ldots + \gamma_n u(u-1)\ldots(u-n-1)\Delta_x^n,$$

and let $\Delta f(x) = f(x + \Delta_x) - f(x) = F(u+1) - F(u)$, then

$$\Delta f(x) = \Delta_x[\gamma_1 + 2\gamma_2 u\Delta_x + \ldots + n\gamma_n u(u-1)\ldots(u-n-2)\Delta_x^{n-1}]$$

viz.,
$$(u+1)u(u-1)\ldots(u-k+1) - u(u-1)\ldots(u-k) = (k+1)u(u-1)\ldots(u-k+1).$$

Let $\Delta(\Delta f(x)) = \Delta^2 f(x), \ldots, \Delta(\Delta^r f(x) = \Delta^{r+1} f(x)$, then by repetition of this procedure

$$\Delta^2 f(x) = \Delta_x^2[2\gamma_2 + 2.3\gamma_3 u\Delta_x + \ldots + n(n-1)\gamma_n u(u-1)\ldots(u-n-3)\Delta_x^{n-2}]$$
$$\Delta^n f(x) = \Delta_x^n \,.\, n!\,\gamma^n\, n.$$

For abbreviation :

$$\Delta^k f(\beta_1) = \Delta_i^k.$$

Hence $\quad \Delta_i^{k+1} = \Delta_{i+1}^k - \Delta_i^k,$

furthermore

$$f(\beta_1) = \gamma_0$$
$$\Delta_1^1 = \Delta_x \gamma_1$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\Delta_1^k = \Delta_x k!\,\gamma_k$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\Delta_i^n = \Delta_x^n n!\,\gamma_n \text{ (for } i = 1, 2, \ldots) \text{ holds.}$$

Hence *Newton's* formula

$$f(x) = f(\beta_1) + \Delta_1^1 u + \frac{1}{2!}\Delta_1^2 u(u-1) + \ldots + \frac{1}{n!}\Delta_1^n u(u-1)\ldots(u-n+1).$$

The elements Δ_i^k can be calculated very easily by the following scheme :

$$\begin{array}{cccc}
\lambda_1 & & & \\
 & \Delta & & \\
\lambda_2 & & \Delta_1^2 & \\
 & \Delta_2^1 & & \Delta_1^n \\
\lambda_3 & \cdot & & \\
\cdot & \cdot & \Delta_{n-1}^2 & \\
\cdot & \Delta_{n-1}^1 & & \\
\lambda_n & & &
\end{array}$$

The degrees of $f(x)$, $\Delta f(x), \ldots, \Delta^n f(x)$ are decreasing, and the last one is a constant ; so we can use the above scheme also for *extrapolation* to get the value of $f(x)$ for every arbitrary integral value of u, that means for every value $x = \beta_1 + k\Delta_x$, where k is an arbitrary integral number.

CHAPTER VI

MATRICES

The problem of solving a system of linear equations leads to the notion of matrix (see Chapter I) ; moreover it has been shown (see 1-11) that any linear transformation of a vectorspace is completely determined by a matrix. As the linear transformations are of the greatest importance for many branches of mathematics, it has been necessary to develop a theory of matrices of which some basic portions will be explained in this chapter. The notion of matrix has been generalised, the theory has been extended far beyond the modest aims of this book, and is now applied nearly everywhere in Mathematics.

In Chapter I, a matrix has been defined as a rectangular scheme of mn numbers ordered in n rows and m columns. It has been shown later on (see 2-61) that the results of Chapter I, excluding 1-7, are not affected if in place of "numbers", elements of an arbitrary field K are arranged in a rectangular scheme to form a matrix. This generalisation will be used here. If the elements of a matrix A are elements of a field K, then A is said to be a *matrix over the field* K. If A is a matrix over K, it is obviously also a matrix over every extension of K. It is sometimes necessary to extend the field over which the matrices are supposed to be situated. On the other hand it is often necessary to restrict the considerations to matrices the elements of which belong to a certain integral domain Δ in K ; these matrices are called *matrices over* Δ. Thus a matrix over Δ is simultaneously a matrix over K, whereas not every matrix over K is a matrix over Δ. With a few exceptions, the matrices under consideration in this chapter will be square shaped matrices, *i.e.* the number of rows is the same as the number of columns ; this number is said to be the *degree* of the matrix. Thus

$$\mathrm{A} = (\,(a^i{}_k)\,) = \begin{pmatrix} a^1{}_1 \ldots a^1{}_n \\ \ldots\ldots\ldots\ldots \\ a^n{}_1 \ldots a^n{}_n \end{pmatrix} \tag{1}$$

is a matrix* of degree n. The notation (1) is very convenient for general investigations. Throughout this chapter, the elements of a matrix of any degree, denoted by capital letters A,B,C, ..., will be expressed by the corresponding small type with upper and lower indices as in (1), unless the elements are expressly given in a different form.

---

* Instead of brackets, sometimes pairs of vertical double bars are used to denote a matrix.

6-1. *Addition and multiplication of matrices of degree* n.

Let K be a field, *0* its zero, and *1* its unitelement ; let Δ be an integral domain in K (which may be identical with K), A, B, C, ... be matrices over Δ of degree n, and let in particular O be the matrix whose elements are all equal to zero. Using the notation explained just before, one defines *addition* and *subtraction* by the following formulas

$$A + B = S, \text{ when } a^i_k + b^i_k = s^i_k \tag{1}$$

$$A - B = D, \text{ when } a^i_k - b^i_k = d^i_k \tag{2}$$

$$\text{for } i, k = 1, \ldots, n.$$

From these definitions follow directly

$$A + B = B + A \qquad \textit{commutative law,} \tag{3}$$

$$(A + B) + C = A + (B + C) \quad \textit{associative law,} \tag{4}$$

$$A + O = O + A = A,$$

and denoting

$$O - B = - B,$$

$$A + (- B) = A - B.$$

Thus addition and subtraction are inverse operations. The matrix $-B$ has the elements $-b^i_k$, and the set of all the matrices over Δ of degree n forms a *module* of which O is the zero-element. The elements of this module can be multiplied with the elements of Δ by the help of the following definition

$$c\,A = (\,(c\,a^i_k)\,). \tag{5}$$

Thus to multiply the matrix A with an element c of Δ, one has to multiply every element of A with c. From (5), the following formulas are immediate consequences :

$$\left.\begin{aligned}(c + d)A &= c\,A + dA \\ c(A + B) &= c\,A + c\,B\end{aligned}\right\} \quad \textit{distributive laws} \tag{6}$$

$$0\,A = O, \quad 1\,A = A, \quad 2\,A = A + A, \quad m\,A = A + \ldots + A. \tag{7}$$

In (7), m denotes an element of the primefield of K which is obtained by repeated addition of *1* to itself (see 2-25). All these elements belong to Δ as Δ is an integral domain ; on the other hand, all these elements m belong to the primefield of K (no restriction has been made for the characteristic of K). Denote by

$$E_{rs} \tag{8}$$

the matrix of degree n, the elements of which are each equal to *0*, except the common element of the r^{th} row and the s^{th} column which is supposed to be equal to *1*.

Then

$$A = \Sigma a^i_k \, E_{ik}. \tag{9}$$

The representation (9) of a matrix A is unique. The left side of (9) is O if and only if the n^2 elements a^i_k are equal to zero each. Hence the n^2 matrices (8) are independent over Δ, and they therefore form a basis. Let Δ be a field ($\Delta = K$), then the matrices form a vectorspace over K (see 2-61). Hence

Theorem 1. The matrices over K of degree n form a vectorspace of rank n^2 over K. The matrices (8) form a basis of that vectorspace.

The *multiplication* of matrices of degree n has been defined already in 1-(11) 1 by

$$A\,B = G \tag{10}$$

if $g^i_k = \sum_j a^i_j \, b^j_k$. That the *associative law*

$$(AB)C = A(BC) \tag{11}$$

holds for this multiplication, has been proved already in 1-(11)1, (3). That the *commutative law is not satisfied* by the multiplication (10), is seen e.g. from the example of the two matrices

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$

which are obviously non-commutative. From (1) and (10) follow easily the *distributive laws*

$$\left.\begin{aligned} A(B + C) &= AB + AC \\ (A + B)C &= AC + BC. \end{aligned}\right\} \tag{12}$$

Using the notation introduced in 2-16, one gets :

Theorem 2. The matrices over Δ of degree n form a ring $R(\Delta, n)$.

The zero-element of $R(\Delta, n)$ is O, its unitelement E is the diagonal-matrix (see p.46), with diagonal-elements equal to *1*. $R(\Delta, n)$ contains a subring Δ' which consists of those diagonal-matrices in which all the diagonal-elements are equal. By mapping each of these matrices on its diagonal-element, one gets an isomorphism between Δ' and the integral domain Δ. The elements of Δ' are commutative with every matrix A of $R(\Delta, \mathrm{n})$. The multiplication (5) of A with an element c of Δ can be replaced by the multiplication of A with the matrix of Δ' which corresponds to c. The matrices of Δ' are sometimes called "scalars", but this notation will not be used here. Let A be a matrix of $R(\Delta, \mathrm{n})$, then one can form "powers" $\mathrm{E} = \mathrm{A}^0$, $\mathrm{A} = \mathrm{A}^1$, $\mathrm{AA} = \mathrm{A}^2, \ldots, \mathrm{A}^k \mathrm{A} = \mathrm{A}^{k+1}, \ldots$ and it follows from the associative law that $\mathrm{A}^r \mathrm{A}^s = \mathrm{A}^{r+s} = \mathrm{A}^s \mathrm{A}^r$ holds. Hence

$$\mathrm{E}, \mathrm{A}, \mathrm{A}^2, \ldots, \mathrm{A}^k, \ldots \tag{13}$$

form a system of matrices which are commutative one to another.

Denote by A and B (with or without indices), matrices of $R(\Delta, \mathrm{n})$, and correspondingly c, d elements of Δ, then $d\mathrm{E} = \mathrm{D}$ belongs to Δ' and therefore

$$c\mathrm{A}d\mathrm{B} = c\mathrm{ADB} = c\mathrm{DAB} = (cd)\mathrm{AB}.$$

More generally

$$\Sigma c_i \mathrm{A}_i \, \Sigma d_j \mathrm{B}_j = \Sigma\, (c_i\, d_j)\mathrm{A}_i\, \mathrm{B}_j$$

$$\Sigma d_j \mathrm{B}_j \, \Sigma c_i \mathrm{A}_i = \Sigma\, (c_i\, d_j)\mathrm{B}_j\, \mathrm{A}_i.$$

If therefore each A_i is commutative with each B_j, then $\Sigma c_i \mathrm{A}_i$ and $\Sigma d_j \mathrm{B}_j$ are also commutative. Hence $c_0 \mathrm{E} + c_1 \mathrm{A} + \ldots + c_m \mathrm{A}^m$ and $d_0 \mathrm{E} + d_1 \mathrm{A} + \ldots + d_r \mathrm{A}^r$ are commutative. Let now

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m$$

run over all the polynomials of $\Delta[x]$, then

$$f(\mathrm{A}) = a_0 \mathrm{E} + a_1 \mathrm{A} + \ldots + a_m \mathrm{A}^m \tag{14}$$

runs over a system of matrices of degree n which form a *commutative subring* $R(\Delta, \mathrm{A})$ of $R(\Delta, \mathrm{n})$. Since $R(\Delta, \mathrm{n})$ has a basis of n^2 elements, the elements (13) cannot be independent. Hence there exists a polynomial $f(x)$ which is different from the zero-polynomial such that

$$f(\mathrm{A}) = \mathrm{O}.$$

A is therefore a *root* of a polynomial, but it is not necessarily a root of a polynomial which is irreducible in $\Delta[x]$, as $f_1(\mathrm{A})\, f_2(\mathrm{A}) = \mathrm{O}$ does not imply that $f_1(\mathrm{A})$ or $f_2(\mathrm{A})$ is equal to O. Although $R(\Delta, \mathrm{A})$ is a commutative ring containing the unitelement E, it might not be an integral domain.

If two fields Δ_1 and Δ_2 have the same primefield, the rings $R(\Delta_1, \mathrm{n})$ and $R(\Delta_2, \mathrm{n})$ have the same zero-element O and the same unitelements E. When different zero or unitelements are considered simultaneously (*e.g.* in 6-21), a proper distinction by indices will be made ; otherwise the notations O and E will be applied.

6-11. *The group* G(K,n). If $\mathrm{n} > 1$, the ring $R(\Delta, \mathrm{n})$ cannot be mapped isomorphically on Δ, as Δ is an integral domain, and $R(\Delta, \mathrm{n})$ is non-commutative. There exists however a non-isomorphic mapping for which the multiplication is invariant but the addition is not. The mapping is

$$\mathrm{A} \rightarrow \det \mathrm{A}. \tag{1}$$

Indeed it has been shown in 1-(11)3 that

$$\det(\mathrm{AB}) = \det \mathrm{A} \det \mathrm{B}.$$

The matrices of rank $< \mathrm{n}$ are mapped on 0, whereas the matrices of rank n are mapped on the elements $\neq 0$ of Δ. Consider now the case when Δ is a field K. The matrices of $R(\mathrm{K}, \mathrm{n})$ having rank n are mapped on the elements $\neq 0$ of the field K. These elements of K form a multiplicative abelian group (see 2-12), as the product of any two elements $\neq 0$ of K is again such an element, and the multiplication is commutative, associative and satisfies the law of inverse existence. The system $G(\mathrm{K,n})$ of the matrices which are mapped on that abelian group has similar properties, only the multiplication is not commutative. To characterise the nature of that system the following definition will be used.

Definition. A system G of elements is said to be a *group* if every ordered pair of elements a, b of G can be composed to an element ab of G and the composition satisfies the following conditions : 1. The composition is associative. 2. There exists an element e in G (the unitelement) such that $ae = a = ea$ holds for every element a of G. 3. To every element a of G, there corresponds an (inverse) element a^{-1} of G such that $aa^{-1} = e = a^{-1}a$ holds.

There cannot exist more than one unitelement in G, for if e and e' are unitelements, ee' must be equal to e and to e'. Moreover there exists only one inverse element, because $ba = e$ implies $baa^{-1} = ea^{-1}$ and therefore $b = a^{-1}$. Similarly one sees that $ax = b$ has, for given a and b, one and only one solution namely $x = a^{-1}b$. Correspondingly $y = ba^{-1}$ is the only solution of $ya = b$.

In the particular cases when the composition is commutative, the conditions (4m), (5m), (6m) of 2-11 are satisfied; if one uses the sign of addition in place of the sign of multiplication, those three formulas are transformed into (4a), (5a), (6a). An additive commutative group is therefore a module; on the other hand every module is obviously an additive commutative group. This justifies the notation "abelian group" introduced in 2-12. The terms "abelian group" and "commutative group" are of course synonymous. Thus the notion of group which has been introduced here appears to be a generalisation of the "abelian group" (module) which has been very often used in the earlier chapters. A more comprehensive study of the fundamental notion of group, is expected to be given in the second volume of this book.

Theorem. The system $G(K,n)$ of the matrices over the field K of degree n and with determinant $\neq 0$ is a group, the matrix multiplication being the composition.

Proof. That the matrix multiplication is associative, and that there exists a unitelement, namely E, has already been proved. It suffices therefore to show the existence of an inverse element, A^{-1} satisfying

$$A\ A^{-1} = E = A^{-1}\ A, \tag{2}$$

but it has been shown already in 1-(11)4 that when A^i_k denotes the cofactor of a^i_k in A, and $b^i_k = A^k_i : \det A$, then $B = A^{-1}$ satisfies (2). Hence the theorem.

From $(AB)\ B^{-1}\ A^{-1} = E$, it follows that

$$B^{-1}\ A^{-1} = (AB)^{-1}. \tag{3}$$

Thus to form the inverse of a product, one has to put the inverse values of its factors, but in the opposite order.

*6-12. *The ring $R(\Delta)$.* The operations of addition and multiplication as defined in 6-1, (1) and (10) cannot be applied without restrictions to non-square shaped matrices. To apply 6-1, (1), one must suppose that the two matrices A and B have the same number of rows, and that they have the same number of columns, which may be different from the number of rows. Moreover 6-1,(10) can be applied if and only if the number of the rows of A is equal to the number of the columns of B; both the conditions cannot hold simultaneously, unless the two matrices are square shaped and of the same degree. This difficulty can be overcome to a certain extent by a method similar to that applied for the addition and multiplication of polynomials (see 2-32). It may be remembered that one is allowed to add higher terms with zero-coefficients to a polynomial $f(x)$, or one may omit such terms, and that this operation does not alter $f(x)$. Similarly one may supplement a matrix by putting some rows composed of zeros below it, and similarly extending it to the right side by columns of zeros ; all these matrices may be considered to be equivalent. In doing so, one replaces the investigation of the matrices by that of classes of matrices, which differ only by zero-rows (below) and zero-columns (on the right side). An equality of matrices defined in this manner, obviously satisfies the conditions for equivalence 2-12.

---

*May be omitted at a first reading.

Let now A and B be two matrices over Δ ; by adding zero-rows and zero-columns one can extend them to square shaped matrices A′ and B′ of a sufficiently high degree, say n′ and to square shaped matrices A″ and B″ of any degree $n'' > n'$. Let

$$\begin{aligned} A' + B' &= S', \qquad & A'B' &= G' \\ A'' + B'' &= S'' & A''B'' &= G'', \end{aligned} \tag{1}$$

then one gets S″ by adding $n'' - n'$ rows below and the same number of columns on the right side to S′, and in the same manner one gets G″ from G′. Thus (1) defines the addition and the multiplication of classes of rectangular matrices of any number of rows and columns, the result being independent of the choice of the square shaped representatives A′ and B′ of the two classes. As addition and multiplication defined in this manner satisfy (3), (4), (11) and (12) of 6-1, *these classes form a ring* $R(\Delta)$. This ring is non-commutative and does not contain a unitelement, though to every element of the ring there exist unities reproducing it (but not every element of $R(\Delta)$) by multiplication. Let *e.g.* α, β and γ be the elements of $R(\Delta)$ which are represented by the matrices

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

respectively. Then $\alpha\gamma = \gamma\alpha = \alpha$,

whereas
$$\beta\gamma = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \text{ and } \gamma\beta = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

It seems to be reasonable to overcome this difficulty by extending every finite matrix to an (enumerably) infinite matrix by adding zero-rows and zero-columns, and to consider matrices with an (enumerable) infinity of rows and columns only. The infinite diagonal-matrix where all the diagonal-elements are equal to I is a unitelement in this system. This procedure shows much analogy to the step leading from polynomials to power series, and as in the theory of power series, considerations about convergence become necessary here. Investigations on infinite matrices and the corresponding vectorspaces however lie beyond the scope of this book.

6-13. *Notations and formulas.* A matrix can be subdivided by horizontal and vertical lines into smaller arrays, and these again can be considered as matrices (sub-matrices) and denoted by capital letters. This procedure will be applied here to square shaped matrices only, and as a matter of convenience, the intersection by horizontal lines is supposed to be symmetric to the intersection by vertical lines; thus *the matrices in the diagonal are always supposed to be square shaped.*

It is not always convenient to give a particular notation to each element or to each submatrix in the array of a matrix. Portions left empty will be considered to be filled with zeros, whereas those portions which are marked with asterisks are occupied by elements of any kind (zeros or non-zeros). Using these notations, one gets the following formulas immediately from the definition of multiplication.

$$\begin{pmatrix} A_1 & * & * \\ & \ddots & * \\ & & \ddots * \\ & & A_s \end{pmatrix} \begin{pmatrix} B_1 & * & * \\ & \ddots & * \\ & & \ddots * \\ & & B_s \end{pmatrix} = \begin{pmatrix} A_1 B_1 & * & * \\ & \ddots & * \\ & & \ddots * \\ & & A_s B_s \end{pmatrix} \tag{1}$$

$$\begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_s \end{pmatrix} \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_s \end{pmatrix} = \begin{pmatrix} A_1 B_1 & & \\ & \ddots & \\ & & A_s B_s \end{pmatrix} \tag{2}$$

$$\begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_s \end{pmatrix} \begin{pmatrix} A_1^{-1} & & \\ & \ddots & \\ & & A_s^{-1} \end{pmatrix} = E \tag{3}$$

In these formulas matrices with the same index are supposed to be of the same degree (which in particular may be equal to 1). Denote the two matrices on the left side of (2) by A and B respectively, then

$$B^{-1}AB = \begin{pmatrix} B_1^{-1}\,A_1\,B_1 & & \\ & \cdot & \\ & & B_s^{-1}\,A_s\,B_s \end{pmatrix} \tag{4}$$

If one interchanges the rows and columns of a matrix, say A, one gets the *transposed* of A, denoted by

$$A^T = \begin{pmatrix} a^1{}_1 & \ldots & a^n{}_1 \\ \ldots & \ldots & \ldots \\ a^1{}_n & \ldots & a^n{}_n \end{pmatrix}. \tag{5}$$

Apply a notation introduced in 1-(11)11

$$(x) = \begin{pmatrix} x_1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ x_n & 0 & \ldots & 0 \end{pmatrix} \tag{6}$$

$$(x)^T = \begin{pmatrix} x_1 & \ldots & x_n \\ 0 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & 0 \end{pmatrix}.$$

These matrices are very useful for representing n-vectors. For abbreviation, (x) is often called a *column-vector*, and $(x)^T$ a *row vector*.

Let A and B be matrices over a field K and of degree n, let B be also of rank n, then B^{-1} exists, and

$$A' = B^{-1}AB \tag{7}$$

is also a matrix over K of degree n. A′ is said to be the *transform* of A by B and to be *similar* to A. This will be denoted by

$$A' \sim A. \tag{8}$$

Similarity satisfies the conditions for "equivalence" (see 2-13). Indeed $A = E^{-1}AE \sim A$ (law of reflexivity). (7) implies $A = BA'\,B^{-1}$, hence $A \sim A'$ (law of symmetry). (7) and $A'' = C^{-1}\,A'C$ together imply $A'' = (BC)^{-1}\,A(BC) \sim A$ (law of transitivity). Hence similar matrices form *classes*.

Let $f(x) = a_0 + a_1 x + \dots + a_n x^n$, and $f(A) = O$, then $O = B^{-1} f(A) B = B^{-1} a_0 EB + B^{-1} a_1 AB + \dots + B^{-1} a_n A^n B = f(B^{-1} AB)$. Hence

Theorem. If A is a root of a polynomial, the matrices similar to A are roots of the same polynomial.

In some respect, the properties of the classes of similar matrices are more interesting than the matrices themselves as it will be seen from the following pages.

6-2. *Transformation of vectorspaces.*

Let W be a vectorspace of rank n over the field K (see 2-61), and let

$$\varepsilon_1, \dots, \varepsilon_n \tag{1}$$

be a basis of W. Then every element of W can be expressed by

$$x_1 \varepsilon_1 + \dots + x_n \varepsilon_n, \tag{2}$$

where $x_1, \dots, x_n$ are elements of K. Thus every element of W can be represented by an n-vector $(x_1, \dots, x_n)$ as considered in Chapter I, but this representation depends on the choice of the basis (see 2-61). If (1) is selected as the basis, then the vectors ε_i are represented as unit-n-vectors, but if a different system of n independent vectors is chosen, then the vectors of the new basis are represented by unit-n-vectors. Let e.g.

$$\beta_1, \dots, \beta_n \tag{3}$$

be another basis of W, where

$$\beta_k = \sum_i b^i_k \varepsilon_i, \tag{4}$$

then the elements b^i_k belong to K, and they form a matrix B, with

$$\det B \neq 0. \tag{5}$$

On the other hand (5) implies the independence of the vectors (3); hence (5) is the necessary and sufficient condition for (3) forming a basis of W. Every vector of W can be represented as a linear function of the basis (1) as well as of the basis (3). Compare the coefficients of these functions, *i.e.* the coordinates of the representing n-vectors.

$$\sum_i x_i \varepsilon_i = \sum_k y_k \beta_k = \sum_{k,i} b^i_k y_k \varepsilon_i.$$

As the vectors ε_i are independent, for $i = 1, \ldots, n$,

$$x_i = \sum_k b^i_k \, y_k$$

holds. Again every n-vector can be represented by a column-vector* (see 6-13, (3)). Thus the last equation can be replaced by a matrix equation

$$(x) = B(y) \tag{6}$$

and therefore

$$(y) = B^{-1}\,(x). \tag{6'}$$

From these considerations follows :

Theorem 1. Let (1) and (3) be two bases of the same vectorspace W, and let them be interconnected by (4). If the same vector is represented by (x) in the system (1) and by (y) in the system (3), then (x) and (y) are interconnected by (6) and (6′).

In particular when the basis (1) is used, the vector ε_k is represented by the kth unitvector and β_k by the kth column of the matrix B, whereas when (3) is used, ε_k is represented by the kth column of B^{-1}, and β_k by the kth unitvector.

Consider now a linear transformation **A** of the vectorspace W. By **A**, the vectors forming the basis (1) are transformed into certain other vectors of W, which again can be represented by the basis, say

$$\varepsilon_k \to \alpha_k = \sum_i a^i_k \, \varepsilon_i, \tag{7}$$

then an arbitrary vector $\xi = \sum x_k \, \varepsilon_k$ is transformed into

$$\xi' = \sum_{i,\,k} a^i_k \, x_k \, \varepsilon_i = \sum x'_i \, \varepsilon_i,$$

where

$$x'_i = \sum a^i_k \, x_k. \tag{7'}$$

This formula can be written as an equation between matrices

$$(x') = A(x). \tag{8}$$

Hence, using any particular basis (1), a linear transformation of W can be expressed by (8). On the other hand, if a matrix A over K is given, (8) determines a linear transformation of W (see 1-11). If in particular det A $\neq 0$, the vectorspace is mapped on itself, and there exists an inverse operation to **A** which is itself a linear transformation. If det A $= 0$, then W is mapped on a subspace W' whose rank is equal to rank A. If one uses a different basis, say (3), then ξ is represented as an n-vector (y) and ξ' by (y'). From (6) and (8) it follows

---

* Instead of using column-vectors, one can represent the n-vectors by row-vectors $(x)^T$ and $(y)^T$ which are interconnected by $(x)^T = (y)^T B^T$.

$$(x) = \mathrm{B}(y),\ (x') = \mathrm{B}(y') = \mathrm{A}(x) = \mathrm{AB}(y).$$

Therefore
$$(y') = \mathrm{B}^{-1}\mathrm{AB}(y). \tag{9}$$

Hence

Theorem 2. If, under the suppositions of theorem 1, the linear transformation **A** of W is expressed by (8) when the vectors are represented by the help of the basis (1), then **A** is expressed by (9) when the same vectors are represented by the help of (3).

Again, let (1) denote any n independent vectors of W, then a linear transformation **A** is uniquely determined by the transformation of vectors (1). By comparing the formulas (7) and (7′) and putting $a^i_k = c^k_i$ one obtains therefore immediately

Theorem 3. If by a linear transformation **A**, a set of n independent vectors (1) is transformed.

$$\varepsilon_i \longrightarrow \Sigma\, c^i_k\, \varepsilon_k,$$

then the transformation **A** is represented by the transposed matrix C^T when (1) is used as the basis.

If in (9), B runs over all the matrices over K of degree and rank n, then (3) runs over all the bases of W, and $\mathrm{B}^{-1}\mathrm{AB}$ over all the matrices similar to A (see 6-13). Thus to a linear transformation **A** there does not correspond a single matrix A, but the full class of similar matrices. On the other hand, a matrix, say A does not correspond to a single linear transformation **A**, as it generates different transformations, according to the different bases used for it. Of course the matrix A generates **A** if the basis (1) is used; if however a different basis, say (3) is used, A generates the same linear transformation as is generated by the matrix $\mathrm{B\,A\,B}^{-1}$ in connection with the basis (1). The matrices which represent this transformation by the help of all possible bases, are the matrices which are similar to A. Thus they form the same class of matrices, as those which represent **A**. Hence there is a (1, 1)-correspondence between the classes of similar matrices and classes of linear transformations, but a correspondence between single matrices and transformations needs the distinction of a particular basis. This interconnection shows the importance of the notion of similarity of matrices.

Let **A** and **B** be two linear transformations which, by help of basis (1), are represented by A and B respectively. Suppose that when ξ runs over the vectorspace W,

$$\mathbf{A} : \xi \rightarrow \xi_1, \quad \mathbf{B} : \xi \rightarrow \xi_2, \quad \xi_1 \rightarrow \xi_3.$$

Then one gets linear transformations $\xi \rightarrow \xi_3$ to be denoted by

$$\mathbf{B}\,\mathbf{A}, \tag{10}$$

and (for any pair a, b of elements of K) $\xi \rightarrow a\xi_1 + b\xi_2$ called

$$a\,\mathbf{A} + b\,\mathbf{B}. \tag{11}$$

When the basis (1) is used, (10) is represented by BA, and (11) by aA + bB. The linear transformations of W therefore form a ring by using any particular basis, this ring is mapped isomorphically to R(K,n). Different bases furnish in general different isomorphisms. The unitelement corresponds to E, whatever basis may be used, and it is therefore denoted by **E**.

6·21. *Permutations as linear transformations.* Let

$$\pi, = \begin{pmatrix} 1, & \ldots, & n \\ a_1, & \ldots, & a_n \end{pmatrix} \tag{1}$$

be a permutation of n objects as considered in (0·3). Then there exists a linear transformation of a vectorspace of rank n over **K** which interchanges the vectors of a particular basis $\varepsilon_1, \ldots, \varepsilon_n$, correspondingly.

$$\varepsilon_k \rightarrow \varepsilon_{a_k} \tag{2}$$

for k = 1, ..., n . Then $\Sigma\, x_k\, \varepsilon_k \rightarrow \Sigma\, x_k\, \varepsilon_{a_k} = \Sigma\, x'_j\, \varepsilon_j$, where

$$x'_{a_k} = x_k, \qquad \text{since } a_k = \mathrm{j}.$$

Hence

$$(x') = \mathrm{P}(x), \qquad \text{where} \tag{3}$$

$$\mathrm{P} = (\,(p^i_k)\,), \text{ and } p^i_k = 1 \quad \text{for } \mathrm{i} = a_k, \quad \mathrm{k} = 1, \ldots, \mathrm{n}$$

$$= 0 \quad \text{for } \mathrm{i} \neq a_k. \tag{4}$$

The matrix P has in every column exactly one element which is equal to *1*, the other elements are equal to *0*. In the k^{th} column, the element *1* stands in the row a_k. As the numbers a_k take every value 1, ..., n once and only once when k runs over 1, ..., n, there is in every row exactly one element which is equal to *1*. Let now Q be any matrix of degree n which shows in every row and in every column exactly one element *1* the other places all being occupied by zero-elements ; if in the k^{th} column, the element *1* stands on the place b_k, then $b_1, \ldots, b_n$ form a permutation of 1, ..., n. Hence the permutation $\xi_k \to \xi_{b_k}$ of the basis is effected by the linear transformation $(x') = Q(x)$. Thus the matrices which have in every row and in every column one element equal to *1* and all other elements equal to *0* are exactly those which effect a permutation of the corresponding basis. If one computes det P as the sum of n! products of elements taken of n different rows and n different columns, one finds that only one of these products is different from *0*.

$$\det \mathrm{P} = \pm \prod p^{a_k}{}_{k} = \pm 1. \tag{5}$$

Let in particular P represent a transposition (i, k), then $p^i{}_k = p^k{}_i = 1$, and $p^j{}_j = 1$, for $i \neq j \neq k$, whereas the other elements are zeros. In this case, $\det \mathrm{P} = -1$. Consider now 2 permutations of the same basis :

$$\pi_1 = \begin{pmatrix} k \\ a_k \end{pmatrix} \quad \text{and} \quad \pi_2 = \begin{pmatrix} j \\ b_j \end{pmatrix}$$

and let P and Q be the corresponding matrices, as above. Perform at first π_1 and then π_2 (see p. 4), then one gets the permutation $\pi_2 \pi_1 = \begin{pmatrix} k \\ b_{a_k} \end{pmatrix}$ which transforms $\varepsilon_k \to \varepsilon_{b_{a_k}}$.

Let $(x'') = Q(x')$, then $x''_{b_j} = x'_j$. Hence

$$(x'') = QP(x) \quad \text{and} \quad x''_{b_{a_k}} = x_k.$$

Thus the composition of two permutations corresponds to the composition of the matrices representing them. The theory of permutations appears to be a special case of the theory of matrices; every even (odd) permutation is composed of an even (odd) number of transpositions ; the determinant of a matrix corresponding to a transposition is equal to -1. Hence a permutation is even or odd according as its determinant is equal to $+1$

or -1. As a corrollary of the preceding considerations, one finds that the two products of two matrices of degree n which have in every row and every column exactly one element equal to 1, the other elements being 0, are matrices of the same type. It is easy to see that these n ! matrices form a group (see 6-11).

Again consider the matrix P representing the permutation π_1 of the basis-vectors $\varepsilon_1, \ldots, \varepsilon_n$. The same transformation of the vectorspace is represented by $B^{-1}PB$ if the basis 6-2.(3) is used. In general, this matrix does not represent a permutation, as the vectors of the new basis will not be interchanged by the transformation, but transformed into other vectors ; if however the two bases differ by the order of the vectors only, $B^{-1}PB$ represents the permutation of the vectors

$$\varepsilon_{b_1}, \ldots, \varepsilon_{b_n}. \tag{6}$$

E.g. one can select B in such a way that the different cycles which constitute the permutation π_1 form sets of consecutive indices of (6). Let $b_1, \ldots, b_r$ form a cycle, then

$$B^{-1}P\,B = \begin{pmatrix} C & O \\ O & * \end{pmatrix}, \text{ where}$$

$$C = \begin{Vmatrix} 0 & & & 1 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{Vmatrix} \text{ is a matrix of degree r.} \tag{7}$$

If B is arranged according to its cycles and the number of the cycles is m, then

$$B^{-1}\,P\,B = \begin{Vmatrix} C & & & \\ & \ddots & & \\ & & \ddots & \\ & & & C \end{Vmatrix} \tag{8}$$

where the C's are matrices of the type (7).

Example
$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} = (1,4) \quad (3,2,5).$$

$$\text{Hence } \mathrm{P} = \left\| \begin{matrix} 0&0&0&1&0 \\ 0&0&1&0&0 \\ 0&0&0&0&1 \\ 1&0&0&0&0 \\ 0&1&0&0&0 \end{matrix} \right\| .$$

To have the cycles formed by consecutive digits, one has to interchange 2 and 4. Hence put

$$\mathrm{B} = \left\| \begin{matrix} 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&0&1&0&0 \\ 0&1&0&0&0 \\ 0&0&0&0&1 \end{matrix} \right\| = \mathrm{B}^{-1}.$$

Then $$\mathrm{B}^{-1}\,\mathrm{PB} = \begin{pmatrix} \mathrm{C}_1 & \\ & \mathrm{C}_2 \end{pmatrix},$$

$$\text{where } \mathrm{C}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathrm{C}_2 = \begin{pmatrix} 0&0&1 \\ 1&0&0 \\ 0&1&0 \end{pmatrix}.$$

Again, consider (8). If $\mathrm{G}_i^{-1}\,\mathrm{C}_i\,\mathrm{G}_i = \mathrm{H}_i$, then it follows from 6·13,(4) that

$$\begin{pmatrix} \mathrm{G}_1 & & \\ & \ddots & \\ & & \mathrm{G}_m \end{pmatrix}^{-1} \begin{pmatrix} \mathrm{C}_1 & & \\ & \ddots & \\ & & \mathrm{C}_m \end{pmatrix} \begin{pmatrix} \mathrm{G}_1 & & \\ & \ddots & \\ & & \mathrm{G}_m \end{pmatrix} = \begin{pmatrix} \mathrm{H}_1 & & \\ & \ddots & \\ & & \mathrm{H}_m \end{pmatrix}.$$

To transform P into a simpler form, it suffices to investigate the transformation of the matrices (7) which correspond to a cyclic permutation of the vectors $\varepsilon_1, \dots, \varepsilon_r$. It is obvious that the vector $\varepsilon_1 + \dots + \varepsilon_r$ is transformed into itself by C. Investigate now whether in the vectorspace V over the field R of the *real numbers* which has the basis $\varepsilon_1, \dots, \varepsilon_r$ there are other vectors $\xi \neq 0$ which are transformed into a vector $\lambda\xi$, where λ is a real number. Let $\xi = z_1\,\varepsilon_1, + \dots + z_r\,\varepsilon_r$, then it follows from (7) that

$$\lambda\, z_1 = z_r$$

$$\lambda\, z_{i+1} = z_i \qquad \text{for } i = 1, \dots, r-1.$$

Hence $\lambda^r = 1$. As λ is supposed to be real, there are two cases

1. $\lambda = 1, \quad \xi = z(\varepsilon_1 + \ldots + \varepsilon_r)$
2. $r = 2m, \quad \lambda = -1, \quad \xi = z(\varepsilon_1 - \varepsilon_2 + \ldots - \varepsilon_{2m})$.

If $\xi \to \pm \xi$, then $\frac{1}{z}\xi \to \pm \frac{1}{z}\xi$, thus the arbitrary factor z can be omitted. Two cases have to be considered now :

1. $r = 2m + 1$. Basis $\gamma_0 = \varepsilon_1 + \ldots + \varepsilon_r$

$$\gamma_i = \varepsilon_i - \varepsilon_{i+1}, \quad \text{for } i = 1, \ldots, 2m.$$

Transformation : $\gamma_0 \to \gamma_0$

$$\gamma_i \to \gamma_{i+1}, \text{ for } i = 1, \ldots, 2m - 1$$

$$\gamma_{2m} \to -\gamma_1 - \gamma_2 \ldots - \gamma_{2m}.$$

$$C \sim H' = \begin{pmatrix} 1 & \\ & L' \end{pmatrix}, \text{ where } L' = \begin{Vmatrix} 0 & & & & -1 \\ 1 & \cdot & & & \cdot \\ & & \cdot & & \cdot \\ & & & \cdot & \cdot \\ & & & & \cdot \\ & & & 1 & -1 \end{Vmatrix}.$$

2. $r = 2m + 2$. Basis $\delta_1 = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_{2m+2}$

$$\delta_2 = \varepsilon_1 - \varepsilon_2 + \ldots - \varepsilon_{2m+2}$$

$$\gamma_i = \varepsilon_i - \varepsilon_{i+1} + \frac{(-1)^i}{m+1}\delta_2, \text{ for } i = 1, \ldots, 2m.$$

Transformation : $\delta_1 \to \delta_1, \ \delta_2 \to -\delta_2$

$$\gamma_i \to \gamma_{i+1}, \text{ for } i = 1, \ldots, 2m - 1$$

$$\gamma_{2m} \to -\sum_1^m \gamma_{2k-1}.$$

$$C \sim H'' = \begin{pmatrix} 1 & & \\ & -1 & \\ & & L'' \end{pmatrix}, \text{ where } L'' = \begin{Vmatrix} 0 & & & & -1 \\ 1 & & & & 0 \\ & \cdot & & & -1 \\ & & \cdot & & \cdot \\ & & & \cdot & \cdot \\ & & & \cdot & \cdot \\ & & & 1 & 0 \end{Vmatrix}.$$

Let **A** be a linear transformation of a vectorspace of rank n over the field R of the real numbers, and let n independent vectors be interchanged by **A**, the permutation being π; suppose π is composed of $r = s + t$ cycles, where s is the number of the odd cycles (which are indeed even permutation !) and t the number of the even cycles. Then one can represent **A** by the matrix (7), and by a further transformation one gets a diagonal-system of matrices where the C's are replaced by H's. From a further transformation which interchanges the basis-vectors only, results the representation

$$\left\| \begin{array}{cccccccccc} E_r & & & & & & & & & \\ & -E_t & & & & & & & & \\ & & L'_1 & & & & & & & \\ & & & \cdot & & & & & & \\ & & & & \cdot & & & & & \\ & & & & & \cdot & & & & \\ & & & & & & L'_\sigma & & & \\ & & & & & & & L''_1 & & \\ & & & & & & & & \cdot & \\ & & & & & & & & & L''_\tau \end{array} \right\| \tag{9}$$

where the unit-matrices E_r and E_t are of the degree of their indices, $\sigma \leqq s$ is the number of the even cycles of more than two elements, and $\tau \leqq t$ the number of the odd cycles of more than one element.

Consider e.g. a 5-dimensional Euclidean vectorspace in which 5-vectors are interchanged by the permutation π_1 as above. Then this transformation can be expressed by

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & -1 & & \\ & & & 0 & -1 \\ & & & 1 & -1 \end{pmatrix}$$

The reader may give a geometrical interpretation to this result.

6-3. *The characteristic polynomial of a matrix.*

Let **A** be a linear transformation of a vectorspace of rank n over a field K. It has been shown already in 6-21 for particular cases that some vectors may be invariant or may take only a factor λ which is an element of K. This question will now be investigated systematically.

Using any particular basis, the transformation **A** is expressed by a matrix A. If a vector $\xi = (x_1, \ldots, x_n)$ is transformed into $\lambda\,\xi$, then $\lambda\xi = A(\xi)$, or, as $\lambda\,\xi = \lambda E\,\xi$,

$$[A - \lambda\, E]\ \xi = O. \tag{1}$$

A vector $\xi \neq O$ with this property exists if and only if the matrix $A - \lambda E$ is of rank $< n$, or

$$\det (A - \lambda E) = 0.$$

Let x be an indeterminate over K, and put

$$\chi_A(x) = \det (A - xE), \tag{2}$$

then $\chi_A(x)$ is a polynomial of $K[x]$, it is said to be the *characteristic polynomial* of A, and the equation $\chi_A(x) = 0$ is called the characteristic equation of A. Hence :

Theorem 1. The necessary and sufficient condition that a linear transformation $\mathbf{A}$, expressed by a matrix A, transforms a vector $\xi \neq O$ into $\lambda \xi$ is that λ is a root of the characteristic polynomial $\chi_A(x)$.

As similar matrices correspond to the same $\mathbf{A}$, it follows already from th. 1 that the characteristic polynomials of similar matrices have the same roots ; it will be shown now that these polynomials are identical. Indeed

$$\begin{aligned} \det (A - xE) &= (\det B)^{-1} \det (A - xE) \det B \\ &= \det [B^{-1}(A - xE)B] = \det (B^{-1} AB - xE). \end{aligned}$$

Hence

Theorem 2. Similar matrices have the same characteristic polynomial.

Thus the characteristic polynomial does not characterise the single matrix but a class of similar matrices, though even these classes are not uniquely determined by their characteristic polynomials. E.g. the matrices $\begin{pmatrix} 1 & \\ * & 1 \end{pmatrix}$ have all the characteristic polynomial $(1 - x)^2$, whereas obviously they are not all similar to each other as the unit-matrix is not similar to any other matrix. It may be remarked that the degree of $\chi_A(x)$ is equal to the degree n of A, and that the highest term has the coefficient $(-1)^n$.

Suppose $\lambda_1, \ldots, \lambda_m$ are *different* roots of $\chi_A(x)$ and $\xi_1, \ldots, \xi_m$ are vectors $\neq O$ for which $A \xi_i = \lambda_i \xi_i$ holds. Suppose the m vectors are dependent, then there exists a subset of them, say $\xi_1, \ldots, \xi_r$ which is dependent, whereas any $r - 1$ of these vectors are independent. There exists therefore one and (up to a common factor) only one equation

$$a_1 \xi_1 + \cdots + a_r \xi_r = O \tag{3}$$

between them. Multiply this matrix equation from the left side with A, then

$$a_1 \lambda_1 \xi_1 + \dots + a_r \lambda_r \xi_r = O. \tag{4}$$

Since the elements λ_i are supposed to be all different, it follows from (3) and (4) that $\xi_1, \dots, \xi_r$ are dependent, contrary to the supposition. The ξ's are therefore independent. Hence

Theorem 3. If $A(\xi_i) = \gamma_i \xi_i$ for $i = 1, \dots, m$ and the m roots λ_i are all different, then the corresponding vectors ξ_i are independent.

6-31. *Characteristic polynomials with* n *different roots.*

Let A be a matrix of degree n over K, and $\chi_A(x)$ its characteristic polynomial. From the fundamental theorem of general algebra (see 2-5) it follows that there exists an algebraic extension Λ of K such that

$$\chi_A(x) = (-I)^n (x - \lambda_1) \dots (x - \lambda_n). \tag{1}$$

Consider now A as a matrix over Λ, and investigate the transformation of the vectorspace V of rank n over Λ by the class of matrices over Λ which are similar to A and correspond to a linear transformation **A**. To every root λ_i, there exists at least one vector $\xi_i \neq O$ in V such that by the transformation **A**

$$\xi_i \rightarrow \lambda_i \xi_i \tag{2}$$

holds. Suppose now that the n roots are all different. Then there exist corresponding to the n different roots also n different vectors ξ_i satisfying (2) and from 6-3, theorem 3 it follows that these vectors are independent; hence they form a basis of V. Every vector α of V can be represented by

$$\alpha = \Sigma x_i \xi_i, \tag{3}$$

and from (2) it follows that $\alpha \rightarrow \Sigma x_i \lambda_i \xi_i$ holds. Hence the transformation **A** is expressed by the matrix

$$L = \begin{pmatrix} \lambda_1 & & & & \\ & \cdot & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \lambda_n \end{pmatrix} \tag{4}$$

when $\xi_1, \dots, \xi_n$ is used as basis of V, and therefore

$$A \sim L. \tag{5}$$

The formula (2) can also be expressed by $L\,\xi_i = \lambda_i\,\xi_i = \lambda_i E\xi_i$. Hence

$$(L - \lambda_i\, E)\, \xi_i = O.$$

$L - \lambda_i\, E$ is a linear polynomial in L, and belongs to the commutative ring $R(\Lambda,\, L)$ (see 6-1); hence these factors are commutative. Therefore

$$\prod_i (L - \lambda_i\, E)\, \xi_j = O, \quad \text{for } j = 1, \ldots, n. \tag{6}$$

From (1) it follows that the product on the left side of (6) is equal to $\chi_A(L)$. Hence $\chi_A(L)$ is a matrix which transforms every vector of the basis, and therefore every vector of V into O. The rank of $\chi_A(L)$ is therefore zero (see 1-5) *i.e.* $\chi_A(L) = O$. Hence L is a root of $\chi_A(x)$; thus it follows from the theorem at the end of 6-13 that

$$\chi_A(A) = O. \tag{7}$$

This formula has been established here under the supposition that the roots of $\chi_A(x)$ are all different, but in 6-32 it will be proved without restriction.

6-32. *Multiple roots of a characteristic polynomial.*

The results of 6-31 must be modified when the characteristic polynomial has multiple roots. The matrix $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ *e.g.* cannot be transformed into a diagonal-matrix, as such a diagonal-matrix is bound to have the same characteristic polynomial as B, *i.e.* it must be the unit-matrix which however is not similar to any other matrix. Moreover it is easily seen that there exists only one 1-dimensional subspace which is invariant for B, whereas when a matrix of degree 2 has a characteristic polynomial with two different roots, two such subspaces exist. The generalisation of the results in 6-31 which will be proved now is the following:

Theorem. Let $\mathbf{A}$ be a transformation of a vectorspace V of rank n over the field Λ, let A be a matrix expressing $\mathbf{A}$, and

$$\chi_A(x) = (\lambda_1 - x)^{r_1} \ldots (\lambda_m - x)^{r_m}, \tag{1}$$

where $\lambda_1, \ldots, \lambda_m$ belong to Λ, then V is generated by m vectorspaces $V_1, \ldots, V_m$ with the following properties (for $j = 1, \ldots, m$):

(1). V_j is of rank r_j and invariant for $\mathbf{A}$.

(2). V_j is transformed into $\mathbf{O}$ by

$$(\mathbf{A} - \lambda\, \mathbf{E})^{r_j} \tag{2}$$

and every vector with this property belongs to V_j.

(3). If $\varepsilon^j_1, \ldots, \varepsilon^j_{r_j}$ is a basis of V_j, then

$$\varepsilon^1_1, \ldots, \varepsilon^1_{r_1}, \ldots \ldots, \varepsilon^m_1, \ldots, \varepsilon^m_{r_m} \tag{3}$$

is a basis of V, and for this basis, **A** is expressed by

$$\begin{pmatrix} L_1 & & \\ & \ddots & \\ & & L_m \end{pmatrix}, \tag{4}$$

where L_j is of rank r_j, and $\chi_{L_j}(x) = (\lambda_j - x)^{r_j}$. Moreover $\chi_A(\mathbf{A}) = \mathbf{O}$.

Proof. As λ_1 is a root of $\chi_A(x)$, there exists a vector, say $\beta_1 \neq O$ which is transformed into $\lambda_1\beta_1$ by **A**. Choose β_1 as the first element of a basis of V, then it follows from 6-2, theorem 3 that **A** is then represented by a matrix

$$A_1 = \begin{pmatrix} \lambda_1 & * \\ & A' \end{pmatrix}, \tag{5}$$

and $A \sim A_1$. The corresponding holds for every matrix of any degree if λ_1 is a root of its characteristic polynomial. Now

$$\chi_A(x) = \chi_{A_1}(x) = (\lambda_1 - x) \det (A' - \lambda x) = (\lambda_1 - x)\ \chi_{A'}(x).$$

Hence

$$\chi_{A'}(x) = (\lambda_1 - x)^{r_1 - 1}\ (\lambda_2 - x)^{r_2} \ldots (\lambda_m - x)^{r_m}.$$

If $r_1 > 1$, then λ_1 is a root of $\chi_A(x)$. Hence A' is similar to a matrix of degree $n - 1$ and of the type (5), say

$$B^{-1} A' B = \begin{pmatrix} \lambda & * \\ & A'' \end{pmatrix}. \text{ Put } B_1 = \begin{pmatrix} 1 & \\ & B \end{pmatrix};$$

from 6-13, (1) it follows that

$$B_1^{-1}\ A_1\ B_1 = A_2 = \begin{pmatrix} \lambda & * & * \\ & \lambda & * \\ & & A'' \end{pmatrix}.$$

and therefore $A \sim A_{r_1}$. This procedure can be repeated r_1 times. The result is

$$A \sim A_{r_1} = \left\| \begin{array}{ccc} \lambda & * \cdots & * \\ & \ddots & \vdots \\ & \lambda & * \\ & & A^{(r_1)} \end{array} \right\|. \tag{6}$$

where $A^{(r_1)}$ is a matrix of degree $n - r_1$. Formula (5) shows that (6) holds also when $r_1 = 1$. Let

$$\beta_1, \ldots, \beta_{r_1}, \gamma_1, \ldots, \gamma_{n-r_1} \tag{7}$$

be the basis of V corresponding to the representation of A by A_{r_1}; then $\beta_1, \ldots, \beta_{r_1}$ generate a vectorspace V_1 of rank r_1 and it will be proved to have the properties stated in the theorem.

(1). A_{r_1} transforms

$$\begin{array}{l} \beta_1 \rightarrow \lambda_1 \beta_1 \\ \beta_2 \rightarrow \lambda_1 \beta_2 + a\beta_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \beta_{r_1} \rightarrow \lambda_1 \beta_{r_1} + c_1 \beta_{r_1-1} + \ldots + c_{r_1-1} \beta_1. \end{array} \tag{8}$$

Hence $\Sigma b_k \beta_k \rightarrow \Sigma d_k \bar{\beta}_k$. V_1 is therefore mapped on itself by A_{r_1}, and as A_{r_1} is the matrix representing **A** for the basis (7), the vectorspace V_1 is invariant for **A**.

(2). From (8) follows that

$$(A_{r_1} - \lambda_1 E)\, \beta_1 = O$$

$$(A_{r_1} - \lambda_1 E)\, \beta_2 = a\, \beta_1\,; \text{ hence } (A_{r_1} - \lambda_1 E)^2\, \beta_2 = O.$$

By repeating this procedure, one gets for $k = 1, \ldots, r_1$

$$(A_{r_1} - \lambda_1 E)^k\, \beta_k = O$$

and therefore $$(A_{r_1} - \lambda_1 E)^{r_1}\, \beta_k = O.$$

Hence $$(A_{r_1} - \lambda_1 E)^{r_1}\; \xi = O,$$

for every vector ξ of V_1, and therefore $(\mathbf{A} - \lambda_1 \mathbf{E})^{r_1}$ maps V_1 on O. Suppose now that there exists in V a vector α which does not belong to V_1 but is mapped on O by a suitable power of $\mathbf{A} - \lambda_1 \mathbf{E}$, say by $(\mathbf{A} - \lambda_1 \mathbf{E})^t$. Consider the sequence of vectors on which α is mapped by $(\mathbf{A} - \lambda_1 \mathbf{E})^k$ for $k = 0, \ldots, t$. The first of these vectors lies outside V_1, the last is O and therefore belongs to V_1. Select the last of the vectors not belonging to V_1 and call it β_{r_1+1}; thus β_{r_1+1} is mapped by $\mathbf{A} - \lambda_1\mathbf{E}$ on a vector of V_1. Now there exists a basis $\beta_1, \ldots, \beta_{r_1}, \beta_{r_1+1}, \delta_1, \ldots, \delta_{n-r_1-1}$ of V. For this basis, $\mathbf{A}$ is represented by

$$C = \begin{pmatrix} \lambda_1 & & & \bullet \\ & \ddots & & \vdots \\ & & \lambda_1 & \bullet \\ & & & S \end{pmatrix},$$

where S is of degree $n - r_1 - 1$.

$C \sim A$. Hence $\chi_A(x) = \chi_C(x)$, but $\chi_C(x) = (\lambda_1 - x)^{r_1+1} \det (S - \lambda_1 E)$, and this contradicts (1). Hence there exists no vector in V outside V_1 which by a suitable power of $\mathbf{A} - \lambda_1\mathbf{E}$ is mapped on O. Hence V_1 has the properties required by (2). In the same manner, one finds subspaces $V_2, \ldots, V_m$ of V with the properties (1) and (2).

(3). To show that $V_1, \ldots, V_m$ generate V, and that a basis $\varepsilon^1_1, \ldots, \varepsilon^m_{r_m}$ as required exists, one has to show that

$$\xi_1 + \ldots + \xi_m = O \tag{9}$$

implies $\xi_1 = \ldots = \xi_m = O$, when ξ_i belongs to V_i (for $i = 1, \ldots, m$). For this purpose, consider the polynomials $\psi_i(x) = \chi_A(x) : (\lambda_i - x)^{r_i}$. The h. c. f. of these m polynomials is of degree 0. Hence (see 2-47, theorem 2) there exist in $\Lambda[x]$ polynomials $k_1(x), \ldots, k_m(x)$ such that

$$\psi_1(x)\ k_1(x) + \ldots + \psi_m(x)\ k_m(x) = I.$$

Hence

$$\psi_1(A)\ k_1(A) + \ldots + \psi_m(A)\ k_m(A) = E. \tag{10}$$

Since for $i \neq j$, $\psi_i(A)$ is divisible by $(A - \lambda_j E)^{r_j}$, there is $\psi_i(A)\ \xi_j = O$. By multiplying (10) with ξ_j from the right side, one gets therefore $\psi_j(A)\ k_j(A)\ \xi_j = \xi_j$. If in particular the vectors $\xi_1, \ldots, \xi_m$ are those satisfying (9), for every particular j, there is

$$O = \psi_j(A)\ k_j(A)\ \Sigma\xi_i = \psi_j(A)\ k_j(A)\ \xi_i = \xi_j.$$

Hence (9) implies that $\xi_1 = \ldots = \xi_m = O$. Select now in every V_j a basis $\varepsilon^j{}_1, \ldots, \varepsilon^j{}_{r_j}$. Then the n vectors $\varepsilon^1{}_1, \ldots, \varepsilon^m{}_{r_m}$ are independent and since n is the rank of V, they form a basis of V. For the transformation **A**, each of the spaces V_j is invariant ; therefore

$$\varepsilon^j{}_k \rightarrow a_1 \, \varepsilon^j{}_1 + \ldots + a_{r_j} \, \varepsilon^j{}_{r_j}.$$

Therefore, if one selects the basis $\varepsilon^1{}_1, \ldots, \varepsilon^m{}_{r_m}$ to represent the transformation **A**, the matrix must have the form (4). In particular, select $\varepsilon^1{}_1 = \beta_1, \ldots, \varepsilon^1{}_{r_1} = \beta_{r_1}$; then it follows from (8) that

$$L_1 = \begin{pmatrix} \lambda_1 & * & \cdots & * \\ & \cdot & & \vdots \\ & & \cdot & \vdots \\ & & & * \\ & & & \lambda_1 \end{pmatrix};$$

hence $\chi_{L_1}(x) = (\lambda_1 - x)^{r_1}$, but this result is independent of the choice of the basis of V_1. Similarly $\chi_{L_i}(x) = (\lambda_i - x)^{r_i}$, for $i = 1, \ldots, m$. As $\varepsilon^j{}_k$ is transformed into **O** by $(\mathbf{A} - \lambda_j \mathbf{E})^{r_j}$, it is also mapped on **O** by $\chi_A(A)$, and this holds for every j. Hence every vector of V is mapped on zero by $\chi_A(A)$, and therefore $\chi_A(A) = O$. Hence the theorem holds.

6·33. *Transformations with characteristic polynomial* $(\lambda - x)^r$.

In the preceding article, the results of 6·31 have been generalised in three directions. Firstly it has been shown that to each of the *different* roots λ_i of the characteristic polynomial, there corresponds an invariant subspace V_i whose rank is equal to the multiplicity r_i of the root ; V_i is characterised by the property that it is mapped on O by $(\mathbf{A} - \gamma_i \mathbf{E})^{r_i}$. Secondly, the equation $\chi_A(A) = O$ holds unconditionally. Thirdly, every matrix can be transformed into a diagonal system of as many matrices as the characteristic polynomial has different roots, the degrees of these matrices are equal to the multiplicities of the different roots and the characteristic polynomials are $(\lambda_i - x)^{r_i}$. Out of these three items only the second one seems to be a full generalisation of a result of 6·31 (see however 6·35). Consider the first and the third way of generalisation. If $r_i = 1$, then V_i is mapped on O by every positive power of $\mathbf{A} - \lambda_i \mathbf{E}$; in general however one knows only, that V is mapped on O by $(\mathbf{A} - \lambda_i \mathbf{E})^e$ for $e \geqq r_i$, but it is not known whether such a mapping can be performed with $e < r_i$. Of course it will be shown here that different cases must be distinguished. When all the roots of $\chi_A(x)$ are different, A is similar to a diagonal-matrix of which every element is known ; when the roots are not all different, the preceding results show only that A is similar to a matrix consisting of a diagonal system of matrices, and of these matrices only the characteristic polynomials $(\lambda_i - x)^{r_i}$ are known.

To supplement the results of 6·32, it is therefore necessary to investigate the subspaces V_i and the matrices L_i for which $\chi_{L_i}(x) = (\lambda_i - x)^{r_i}$, since when V is transformed by A (using a particular basis), then V_i is transformed by L_i. If on the other hand, one finds a uniquely determined distinguished matrix H_i which is similar to L_i (for $i = 1, \ldots, m$), then A is similar to the matrix formed by the m matrices H_i written in the diagonal. Thus if "canonical" forms for those matrices where the roots of the characteristic polynomial are all equal are found out, one gets automatically canonical forms for all the matrices.

Suppose now that L is a matrix of $R(\Lambda, r)$ let

$$\chi_L(x) = (\lambda - x)^r, \tag{1}$$

where λ belongs to Λ. The corresponding vectorspace of rank r over Λ will be denoted by V. If for any vector ξ of V

$$(L - \lambda E)^e \, \xi = O \tag{2}$$

holds, then the same equation holds for every exponent $k > e$. Let e be the smallest positive integer for which (2) holds, then e is called the *exponent* of ξ,

$$exp\ \xi = e. \tag{2'}$$

Since $(L - \lambda E)^r = (-1)^r \chi_L(L) = O$, $e \leqq r$ for every vector ξ. If there exists a vector η in V such that

$$(L - \lambda E)^h \, \eta = \xi, \tag{3}$$

then the same equation can be satisfied for any non-negative integral exponent $j < h$, as $\eta' = (L - \lambda E)^{h-j} \eta$ implies $(L - \lambda E)^j \eta' = \xi$. Let h be the highest non-negative integer for which (3) holds true, then h is called the *height* of ξ,

$$height\ \xi = h. \tag{3'}$$

Obviously, *height* $\xi < r$ for $\xi \neq O$. Moreover

$$exp\ c\xi \leqq exp\ \xi, \quad \text{height}\ c\,\xi \geqq height\ \xi \tag{4}$$

for every element c of Λ, but inequality holds in (4) only for $c = 0$.

Let *exp* $\xi_1 \leqq k$, *height* $\xi_1 \geqq j$

exp $\xi_2 \leqq k$, *height* $\xi \geqq j$, then for $i = 1, 2$

$$\left.\begin{array}{l}(L - \lambda\ E)^k\ \xi_i = O \\ (L - \lambda\ E)^j\ \eta_i = \xi_i\end{array}\right\} \text{ and therefore } \left\{\begin{array}{l}(L - \lambda\ E)^k\ (\xi_1 \pm \xi_2) = O \\ (L - \lambda\ E)^j\ (\eta_1 \pm \eta_2) = \xi_1 \pm \xi_2\end{array}\right. \tag{5}$$

From (4) and (5) follows :

Lemma 1. The vectors of V with an exponent $\leqq k$ form a vectorspace over Λ say W_k ; the vectors of V with a height $\geqq j$ form a vectorspace over Λ, say W^j.

$$\text{Obviously, } W_g \subseteq W_k \qquad \text{for } g < k$$

$$W^i \subseteq W^j \qquad \text{for } i > j$$

$$W_r = W^0 = V.$$

Consider now any particular transformation, and suppose that $r' \leqq r$ is the greatest exponent which occurs, and h' the highest height of vectors $\neq O$. Then there exists a particular vector η_0 such that

$$(L - \lambda\ E)^{r'-1}\ \eta_0 = \xi_0 \neq O\ ;$$

thus *height* $\xi_0 \geqq r' - 1$; hence $h' \geqq r' - 1$. Moreover there exists a vector $\xi_1 \neq O$ such that

$$(L - \lambda E)^{h'}\ \eta_1 = \xi_1 \neq O\ ;$$

thus *exp* $\eta_1 \geqq h' + 1$; hence $r' \geqq h' + 1$. Hence

$$h' = r' - 1. \tag{6}$$

Let $\xi \neq O$, *exp* $\xi = e$, *height* $\xi = h$, then $(L - \lambda\ E)^{e-1}\ \xi \neq O$, *exp*$(L - \lambda\ E)^{e-1}\ \xi = 1$, *height* $(L - \lambda\ E)^{e-1}\ \xi = h + e - 1 \leqq h' = r' - 1$. Hence

$$h' + e \leqq r'. \tag{7}$$

If in particular $e = r'$, then $h = 0$, and *exp* $(L - \lambda\ E)^j\ \xi = r' - j$, *height* $(L - \lambda\ E)^j\ \xi = j$. Hence every exponent between 1 and r' and every height between 0 and $r' - 1$ actually occur. The above inequalities can therefore be replaced by

$$\begin{array}{ll} W_g \subset W_k & \text{for } 0 \leqq g < k \leqq r' \\ W^i \subset W^j & \text{for } 0 \leqq j < i < r'. \end{array} \tag{8}$$

Hence

$$W_1 \subset W_2 \subset \ldots \subset W_{r'} = V$$
$$W^{r'-1} \subset W^{r'-2} \subset \ldots \subset W^0 = V.$$

Denote the meet

$$W_k \cap W^j = W^j_k ; \tag{9}$$

then $W^i_g \subseteq W^j_k$ for $j \leqq i < r'$, $0 \leqq g \leqq k$. The subspaces W_k, W^j, W^j_k are independent of any selection of a basis. The ranks of these spaces are uniquely determined by the transformation **L**, and it will be shown in 6-333 that they suffice to find out a ("canonical") representation of the transformation by a matrix of a particular type ; thus these numbers will prove to be characteristic for **L**. To reach that result, the following lemma will be used.

Lemma 2. If $0 < exp\ \xi_1 < \ldots < exp\ \xi_m$, then $\xi_1, \ldots, \xi_m$ are independent.

Proof. Let the vectors be dependent, then one can suppose without loss of generality, that $\xi_1, \ldots, \xi_s$ are independent, whereas $\xi_{s+1} = \sum_{i=1}^{s} c_i \xi_i$. Put $exp\ \xi_{s+1} = t+1$, then $(L - \lambda E)^t \xi_{s+1} \neq O$, whereas $(L - \lambda E)^t \sum c_i \xi_i = O$. Hence the lemma.

Exercises : (1). Establish a statement on vectors of different heights, analogous to lemma 2.

(2). Consider the exponent of a vector of V as its "measure" and find out the inequalities which hold for the sides of a (degenerate or non-degenerate) triangle ; establish the corresponding inequalities when the vectors are measured by their heights.

(3). Investigate whether corresponding inequalities hold for other mathematical entities and suitable operations, *e.g.* the ring of the polynomials $K[x]$, the ring of the numbers mod. p^r, the system of curves which pass through a particular point P and are differentiable in P to every order.

6-331. *The case* $r' = 1$. In this case, $W_1 = V$. Every vector $\neq O$ is of exponent 1 and of height 0. Let $\beta_1, \ldots, \beta_r$ be any basis, then $(L - \lambda E)\ \beta_i = O$; hence $L\ \beta_i = \lambda\ \beta_i$, for $i = 1, \ldots, r$. Thus the transformation is represented by a diagonal matrix

$$L = \begin{pmatrix} \lambda & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \lambda \end{pmatrix} .$$

whatever basis may be used. In Geometry, this transformation is known as a *similarity* of the r-dimensional space.

6·332. *The case* $r' = r$. Suppose there is such a case, then there exists a vector, say β_r of exponent r. Put $(L - \lambda E)^{r-k}\ \beta_r = \beta_k$ for $k = 1, \ldots, r$, then *exp* $\beta_k = k$, and *height* $\beta_k \geqq r - k$, but as the sum of height and exponent cannot be greater than r (see 6-33 (7)), there is *height* $\beta_k = r - k$. From 6-33, lemma 2 it follows, that the r vectors

$$\beta_1, \ \ldots, \ \beta_r \tag{1}$$

are independent, and therefore they form a basis of V. Now $(L - \lambda E)\beta_k = \beta_{k-1}$, and therefore $L\,\beta_k = \lambda\,\beta_k + \beta_{k-1}$. Thus by **L** the basis is transformed as follows :

$$\begin{aligned}
&\beta_1 \rightarrow \lambda\ \beta_1\\
&\beta_2 \rightarrow \beta_1 + \lambda\ \beta_2\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&\beta_k \rightarrow \beta_{k-1} + \lambda\ \beta_k\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&\beta_r \rightarrow \beta_{r-1} + \lambda\ \beta_r.
\end{aligned}$$

Hence it follows from 6-2, theorem 3 that **L** can be represented by

$$H_r = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \cdot & & \\ & & \cdot & \cdot & \\ & & & \cdot & 1 \\ & & & & \lambda \end{pmatrix}. \tag{2}$$

This formula shows that the case $r' = r$ actually exists, and that for a given number r all the transformations under consideration are similar. Thus there is one canonical form for the matrices in this case, as there is one canonical form for $r' = 1$. Similarly by H_{r_i} a matrix of the type (2) with the characteristic polynomial $\chi_{H_{r_i}}(x) = (\lambda_i - x)^{r_i}$ will be denoted.

Let $\alpha = c_1\,\beta_1 + \ldots + c_r\,\beta_r$, where $c_i = 0$, for $i < r - j$ and for $i > k$, whereas c_{r-j} and c_k are different from 0. Since *exp* $\beta_s = s$, and *height* $\beta_s = r - s$ holds for $s = 1, \ldots, r$, it follows *exp* $\alpha = k$, *height* $\alpha = j$. Hence $\beta_{r-j}, \beta_{r-j+1}, \ldots, \beta_k$ form a basis of W^j_k; in particular $\beta_1, \ldots, \beta_k$ is a basis of W_k^* and $\beta_{r-j}, \ldots \beta_r$ is a basis of W^j. These subspaces have been defined in 6-33 in an invariant manner.

6·333. *Characteristic polynomials with a single root : general case.* Let $r_1 \geqq r_2 \geqq \ldots \geqq r_p > 0$, and $\Sigma\, r_i = r$, then the matrix

$$\begin{pmatrix} H^{r_1} & & & \\ & \cdot & & \\ & & \cdot & \\ & & & H^{r_p} \end{pmatrix} \tag{1}$$

is of degree r, and its characteristic polynomial is $\prod (\lambda - x)^{r_i}$. If $p = r$, then every r_k is equal to 1, and this is the case which was considered already in 6·331, but if $p = 1$, it is the case of 6·332. It will be proved that (1) is the most general case, *i.e.* that every matrix with characteristic polynomial $(\lambda - x)^r$ is similar to one and only one matrix of the type (1). To establish this theorem, it is convenient to construct beforehand the invariant subspaces W^j, W_k, W^j_k and to investigate their properties when a particular transformation **L**, represented by a matrix of type (1), is given. As it has been shown in 6·332, every H^{r_i} can be represented by a basis

$$\beta^1{}_i,\ \beta^2{}_i,\ \ldots,\ \beta^{r_i}{}_i \quad \text{for } i = 1, \ldots, p \tag{2}$$

in such a way that

$$(\mathbf{L} - \lambda\ \mathbf{E})\ \beta^k{}_i = \beta^{k-1}{}_i$$

$$(\mathbf{L} - \lambda\ \mathbf{E})\ \beta^1{}_i = 0. \tag{3}$$

Hence

$$\mathit{exp}\ \beta^k{}_i = k,\ \mathit{height}\ \beta^k{}_i = r_i - k. \tag{4}$$

The $r_1 + \ldots + r_p = r$ vectors $\beta^k{}_i$ form a basis of V. Arrange these vectors in the following manner.

$$\begin{aligned} &1^{st}\ \text{row}: \quad \beta^1{}_1\ \beta^1{}_2, \ldots, \beta^1{}_p. \\ &i^{th}\ \text{column}: \beta^1{}_i, \beta^2{}_i, \ldots, \beta^{r_i}{}_i\ \text{(vertical)}. \end{aligned} \tag{5}$$

E.g. let $r_1 = r_2 = 5$, $r_3 = r_4 = r_5 = 3$, $r_6 = 2$, $r_7 = 1$, then the scheme reads :

$$\begin{matrix} \beta^1{}_1 & \beta^1{}_2 & \beta^1{}_3 & \beta^1{}_4 & \beta^1{}_5 & \beta^1{}_6 & \beta^1{}_7 \\ \beta^2{}_1 & \beta^2{}_2 & \beta^2{}_3 & \beta^2{}_4 & \beta^2{}_5 & \beta^2{}_6 & \\ \beta^3{}_1 & \beta^2{}_2 & \beta^3{}_3 & \beta^3{}_4 & \beta^3{}_5 & & \\ \beta^4{}_1 & \beta^4{}_2 & & & & & \\ \beta^5{}_1 & \beta^5{}_2 & & & & & \end{matrix} \tag{5'}$$

The index of a row shows the exponent, whereas the height is given by the number of β's standing in the same column below the considered vector. The first k rows form a basis of the subspace W_k.

Thus rank W_1 = number of β's in the 1st row.

rank W_k — rank W_{k-1} = number of β's in the kth row.

Hence the shape of the triangular scheme (5) is completely determined by the ranks of the spaces W_k. It is therefore impossible that a transformation is representable by two non-isomorphic matrices of the type (1). Moreover if (5) is a basis of V, and the conditions (3) are satisfied, every column of (5) is a basis of a subspace V_i of rank r_i which is mapped on itself by **L**, the transformation of V_i being represented by H_{r_i}, and therefore the transformation of V by (1). After these remarks it is easy to prove the following theorem.

Theorem. If $\chi_L(x) = (\lambda - x)^r$, then L is similar to one and only one matrix of the type (1).

Proof. It suffices to prove that there exists a basis (5) which satisfies the conditions (3). Let rank $W_1 = p$, and $r' \leqq r$ be the highest exponent occuring in V. Consider the sequence of subspaces $W^{r'-1}_1 \subseteq \ldots \subseteq W^1_1 = W_1$; omit in this sequence all those subspaces which are identical with preceding ones, so getting

$$W^{r'-1}_1 \subset W^s_1 \subset \ldots \subset W^t_1 = W_1, \tag{6}$$

where $r' - 1 > s > \ldots > t \geqq 1$. Construct now a basis

$\beta^1_1, \ldots, \beta^1_a$ of $W^{r'-1}_1$, supplement it to a basis

$\beta^1_1, \ldots, \beta^1_a, \beta^1_{a+1}, \ldots, \beta^1_b$ of W^s_1 and continue this procedure up to it comes out finally as a basis

$$\beta^1_1, \ldots, \beta^1_a, \ldots, \beta^1_b, \ldots \quad \ldots, \beta^1_p \tag{7}$$

of $W^t_1 = W_1$ which has the property that to each W^k_1 there corresponds an initial section of (7) which is a basis of W^k_1. Since the vectors $\beta^1_1, \ldots, \beta^1_a$ are of height $r' - 1$, there exist vectors $\beta^{r'}$ such that, for $\mu = 1, \ldots, a$, $(L - \lambda E)^{r'-1} \beta^{r'}_\mu = \beta^1_\mu$. Put $(\mathbf{L} - \lambda \mathbf{E})^{r'-k} \beta^{r'}_\mu = \beta^k_\mu$, and arrange these vectors into columns as in (5). The row-index k is equal to the exponent of the vector, and the height is equal to $r' - k$, which is equal to the number of vectors standing in the same column below it. Correspondingly, there exist, for $\nu = a + 1, \ldots, b$, vectors β^s for which $(\mathbf{L} - \lambda \mathbf{E})^{s-1} \beta^s_\nu = \beta^1_\nu$; again put $(\mathbf{L} - \lambda \mathbf{E})^{s-k} \beta^s_\nu = \beta^k_\nu$, arrange these vectors in columns as in (5) and continue this procedure up to the end of (7). The triangular scheme obtained in this way satisfies the conditions (3); moreover every row-index shows the exponent and the height is equal to the number of β's standing vertically below. It remains to show that all these β's form a basis of V. If any linear equation holds, it can only be an equation between vectors of the same exponent, *i.e.* between β's of the same row, but if $\sum\limits_j c_j \beta^k{}_j = O$, it follows by multiplication from left side with $(\mathbf{L} - \lambda\ \mathbf{E})^{k-1}$ that $\sum\limits_j c_j \beta^1{}_j = O$. Now the vectors in the first row form a basis of W_1 and are therefore independent. Thus the β's are independent. To show that they generate V, it will be proved by mathematical induction that for $k = 1, \ldots, r'$, the k first rows generate W_k. This statement is true for $k = 1$; suppose it to be true for $k = q - 1$ and let $exp\ \xi = q$. For $\xi' = (\mathbf{L} - \lambda\ \mathbf{E})\ \xi$, $exp\ \xi' = q - 1$; hence $\xi = \sum\limits_{i<q} c_{i,j}\ \beta^i{}_j$. For the same coefficients $c_{i,j}$, put $\sum c_{i,j}\ \beta^{i+1}{}_j = \eta$; then $(\mathbf{L} - \lambda\ \mathbf{E})\ (\xi - \eta) = O$, and therefore $exp\ (\xi - \eta) \leqq 1$. Hence $\xi - \eta$ belongs to W_1, and therefore $\xi - \eta = \sum\limits_k d_k\ \beta^1{}_k$; thus ξ depends on the β's in the q first rows. Hence the theorem.

6-34. *Characteristic polynomials with any number of roots.* The theorems of 6-32 and 6-33 furnish directly the following general result.

Main theorem on similarity of matrices. Every matrix A of $R(\Lambda, n)$ with the characteristic polynomial $\chi_A(x) = (\lambda_1 - x)^{r_1} \ldots (\lambda_m - x)^{r_m}$ is similar to one and only one matrix up to a permutation at the L_μ (*canonical form*)

$$A \simeq \begin{pmatrix} L_1 & & \\ & \ddots & \\ & & L_m \end{pmatrix}, \text{ where } L_j = \begin{pmatrix} H^j{}_1 & & \\ & \ddots & \\ & & H^j{}_{p_j} \end{pmatrix} \qquad (1)$$

$$\text{and } H^j{}_k = \begin{pmatrix} \lambda_j & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_j \end{pmatrix} \text{ for } \quad k = 1, \ldots, p_j,$$

L_j being of degree r_j, $H^j{}_k$ of order $r_{j,k}$, moreover $\sum\limits_k r_{j,k} = r_j$, and $r_{j,1} \geqq r_{j,2} \geqq \ldots \geqq r_{j,p_j}$.

6·341. *Application to the theory of the linear substitutions of a complex variable.* Consider the complex linear substitutions of the type

$$w = \frac{\alpha z + \beta}{\gamma z + \delta}, \text{ where } \alpha\delta - \beta\gamma \neq 0.$$

Introduce homogeneous coordinates $w = w_1 : w_2$, $z = z_1 : z_2$; then

$$w_1 = \alpha z_1 + \beta z_2, \quad w_2 = \gamma z_1 + \delta z_2.$$

As a common complex factor of α, β, γ, δ is arbitrary, one can arrange that $\alpha\delta - \beta\gamma = 1$; now only a common factor ± 1 is arbitrary.

Let $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = A$. $\chi_A(x) = x^2 - \kappa x + 1 = (\lambda_1 - x)(\lambda_2 - x)$.

Hence $\lambda_1 \lambda_2 = 1$, thus $\lambda_1 = r\, e^{i\phi}$, $\lambda_2 = r^{-1}\, e^{-i\phi}$.

Two cases must be distinguished.

(1) $\lambda_1 \neq \lambda_2$, normal-form : $\begin{pmatrix} re^{i\phi} & 0 \\ 0 & r^{-1}e^{-i\phi} \end{pmatrix}$. (1)

As a factor ± 1 and a permutation of λ_1, λ_2 are arbitrary, choose $1 \leqq r$, $0 \leqq \phi < \pi$.

(2) $\lambda_1 = \lambda_2 = 1$, $\kappa = \pm 2$; as a common factor $= \pm 1$ is arbitrary, suppose without loss of generality that $\lambda_1 = \lambda_2 = 1$, $\kappa = 2$. Thus there are two normal-forms

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \qquad (2)$$

These transformations are largely discussed in the elements of the theory of functions. The classes of transformations with the normal-form (1) are said to be *loxodromic*, they have two fixed points, which for the normal-form, are chosen as 0 and ∞. In the particular case where $r = 1$, the transformations are called *elliptic*, and if $r > 1$, $\phi = 0$, *hyperbolic*. The first matrix (2) denotes the identity, the second matrix denotes a *parallel-displacement*, the infinite point of the complex sphere being the only fixed point and the other transformations of this class are called *parabolic* transformations, the only fixpoint being a finite point.

6·35. *Polynomials of which A is a root.* Let $f(x)$ be a polynomial of $\Lambda(x)$, then $f(\mathrm{A})$ is a matrix, and $f(\mathrm{A}) = O$ if and only if this matrix maps V on O, that means: if $f(\mathrm{A})\ \xi = O$ for every vector ξ of V. If $f(x)$ runs over all the polynomials of $\Lambda[x]$, the polynomials $f(\mathrm{A})$ form a commutative ring $R(\Lambda, \mathrm{A})$ (see 6-1); hence $f_1(\mathrm{A}) = O$ implies $f_1(\mathrm{A})\ f(\mathrm{A}) = O$, and if A is a root of $f_1(x)$ and $f_2(x)$, it is also a root of $k_1 f_1(x) + k_2 f_2(x)$, hence it is a root of the highest common factor $(f_1(x), f_2(x))$. In every matrix-equation, the matrix can be replaced by a similar one (see the theorem of 6-13); thus one may replace the matrix by the transformation which it represents, or conversely. Apply now the notations of (6-33).

Every vector ξ of V can be represented by

$$\xi = \xi_1 + \dots + \xi_m, \tag{1}$$

where ξ_i belongs to V_i. Since the vectorspaces V_i are invariant for A, the transformation $\mathbf{A}$ of the vectors ξ_i is represented by L_i. Let now $r^i_1, r^i_2, \dots, r^i_{\nu_i}$ be the degrees of the matrices $\mathrm{H}^i_1, \dots, \mathrm{H}^i_{\nu_i}$ respectively, then

$$(\mathbf{A} - \lambda_i\ \mathbf{E})^{r^i_1}\ \xi_i = O, \text{ for } i = 1, \dots, m, \tag{2}$$

but for every $t < r^i_1$ there exist vectors η_i of V_i such that

$$(\mathbf{A} - \lambda\ \mathbf{E})^{t}\ \eta_i \neq O. \tag{2'}$$

Put $r^i_{\nu_i+1} = r^i_{\nu_i+2} = \dots = 0$, and

$$\varphi_k(x) = \prod_i\ (x - \lambda_i)^{r^i_k} \text{ for } k = 1, \dots, n. \tag{3}$$

Since $r^i_1 \geqq r^i_2 \geqq \dots \geqq r^i_{\nu_i} \geqq 0 = r^i_{\nu_i+\nu}$ holds for every i, in the sequence

$$\varphi_1(x),\ \varphi_2(x),\ \dots,\ \varphi_n(x), \tag{4}$$

every polynomial is divisible by the following one, except in the case when the polynomials (4) are all equal, $\varphi_n(x)$ is the polynomial 1. Moreover

$$\chi_{\mathrm{A}}(x) = \prod_k\ \varphi_k(x). \tag{5}$$

Since from (2) and (3) it follows that $\varphi_1(\mathrm{A})\ \xi_i = O$ for every i, formula (1) shows that $\varphi_1(\mathrm{A})\ \xi = O$ for every ξ of V. Hence

$$\varphi_1(\mathrm{A}) = O. \tag{6}$$

Suppose now that $F(x)$ is a polynomial of $\Lambda[x]$, and let $F(\mathrm{A}) = \mathrm{O}$. Form the *h. c. f.*, say

$$(F(x), (x-\lambda_i)^{r^i_1}) = k_1(x)\ F(x) + k_2(x)\ (x-\lambda_i)^{r^i_1}$$
$$= (x-\lambda_i)^t,$$

then $(k_1(\mathrm{A})\ F(\mathrm{A}) + k_2(\mathrm{A})\ (\mathrm{A} - \lambda_i\ \mathrm{E})^{r^i_1})\ \eta_i = (x - \lambda_i\ \mathrm{E})^t\ \eta_i$.

The left side is equal to O but from (2′) it follows that there exist vectors η_i in V_i such that the right side is different from O when $t < r^i_1$. Hence $F(x)$ is divisible by $(x-\lambda_i)^{r^i_1}$ and — since it holds for every i — divisible by $\phi_1(x)$. From this statement and from (6) follows :

Theorem. $F(\mathrm{A}) = \mathrm{O}$, if and only if $F(x)$ is divisible in $\Lambda[x]$ by $\phi_1(x)$.

If the factorisation (5) of $\chi_{\mathrm{A}}(x)$ into factors $\phi_k(x)$ (of which in general some are reducible, and others are *I*) is given, the roots λ_i and the exponents r^i_k are determined, and these again determine uniquely the canonical form of the matrix. Hence the right side of (5) characterises uniquely the corresponding class of similar matrices (transformations). In the particular case, where the roots of $\chi_{\mathrm{A}}(x)$ are all different, $\chi_{\mathrm{A}}(x) = \phi_1(x)$; thus in this case the class of matrices is uniquely determined by the characteristic polynomial.

Let $\mathrm{K} \supset \Lambda$, and suppose that $\chi_{\mathrm{A}}(x)$ belongs to $\mathrm{K}[x]$; then $\phi_1(x)$ may not belong to $\mathrm{K}[x]$ as it is seen by the example

$$\mathrm{A} = \begin{pmatrix} \sqrt{2} & & & \\ & \sqrt{2} & & \\ & & -\sqrt{2} & 1 \\ & & & -\sqrt{2} \end{pmatrix}.$$

That however $\phi_1(x)$ belongs to $\mathrm{K}[x]$ when A is a matrix over K, will be shown in 6-44.

6-4. *Elementary divisors.*

In 6-2 and 6-3 matrices over a field have been investigated. This section deals with matrices over a *Euclidean* domain Δ ; thus the theory to be developed here can be applied *e.g.* to matrices whose elements are integral numbers as well as to the case when the elements are polynomials in x over a field. The difference between matrices over a field K and matrices over Δ appears from the following comparison.

If A runs over all the matrices of $R(\mathrm{K}, \mathrm{n})$, and $\xi \neq 0$ is a vector of a vectorspace V over K, then $\mathrm{A}\xi$ runs over all the vectors of V; moreover if B is a particular matrix of $R(\mathrm{K},\mathrm{n})$, then it maps V either on itself (namely if $\det \mathrm{B} \neq 0$) or on a subspace of a lower rank. On the other hand, let Δ be a Euclidean domain which is *not* a field, and $\Delta \subset \mathrm{K}$. If A runs over $R(\Delta, \mathrm{n})$, then $\mathrm{A}\,\xi$ runs over the vectors of a modul M of rank n over Δ but M is not a vectorspace; moreover a matrix B of $R(\Delta, \mathrm{n})$ may map M on a submodul which is of the same rank n but not identical with M.

This comparison suffices to show that the transformations to be considered now are of a quite different character to those treated earlier. Correspondingly a different equivalence of matrices will be used here. On place of classes of *similar* matrices, classes of *congruent* matrices will be investigated; it must however be emphasised that—unlike in Geometry—*congruence is not a special case of similarity.* It is better not to think of the geometrical significance of these two words when using them for matrices. Congruence of matrices can be defined either by the help of operations on rows and columns, or by matrix multiplication; both definitions lead to the same result. At first the operations on rows and columns will be used. (See 1-4 and 2-44).

6·41. *Congruent matrices.* Let A be a matrix of the ring $R(\Delta, \mathrm{n})$, and let $\alpha_1, \ldots, \alpha_n$ be its column-vectors. If c is an element of Δ and $\mathrm{i} \neq \mathrm{k}$ then the transformation

$$\alpha_i \to c\ \alpha_k + \alpha_i \tag{1}$$

is called a *column-addition*, whereas $\alpha_i \to c\ \alpha_i$ is a *column-multiplication* with c; correspondingly the terms *row-addition* and *row-multiplication* are used. These definitions tally to a certain extent with those of 1-4. In Chapter I, c was supposed to be a number; in (2-61) the generalisation from "number" to "element of a field K" was performed, but here, c is bound to be an element of a Euclidean domain Δ. If A is transformed into A′ by a row-(or a column) addition, then A′ is transformed into A by a transformation of the same type, c being replaced by $-c$. If however the transformation $\mathrm{A} \to \mathrm{A}'$ is done by row-(column) multiplication, the inverse operation is the division of a row (column) by an element c of Δ, and this operation is a row-(column) multiplication if and only if c is a unity of Δ. A transformation which is composed of zero or more row-additions, column-additions, row-multiplications with unities and column-multiplications with unities, is called a *congruence*. Thus if A is transformed by a congruence into A′, the inverse transformation is also a congruence; *i.e.* congruence satisfies the law of symmetry. That congruence satisfies also the laws of reflexivity and transitivity is obvious. Hence congruence is an equivalence, and one can form classes of *congruent matrices* in R(Δ, n). The congruence of two matrices A and A′ is denoted by

$$A \sim A'. \tag{2}$$

To find out the invariants for classes of congruent matrices, it suffices to determine those properties of a matrix which are invariant for row-(and column) addition as well as for row-(and column) multiplications with unities. The column-addition (1) transforms

$$a^j{}_i \to a^j{}_i + c\, a^j{}_k \quad \text{for } j = 1, \ldots, n,$$

whereas the other elements of A remain unaltered. If therefore d is a common factor of all the elements of A, then it is also a common factor of the elements of the transformed matrix A′; the corresponding holds for row-addition and for row-and column-multiplication. Hence if A′ is congruent to A, every element of A′ is divisible by the *h.c.f.*, say δ_1 of the elements of A but as in this case A is also congruent to A′, the matrices have the same *h.c.f.*(which is determined up to a unity factor only).

This consideration can be generalised to the *h. c. f.*, say of the minors of degree q. Indeed, the elements of A are the minors of degree 1. Let M be a matrix formed by q rows and q columus of A. If the ith column does not contain any element of M, then M is not altered by the column-addition (1); if both the ith and the kth columns have elements in common with M, then M is altered but det M is unchanged; if the ith column, but not the kth column has elements in common with M, and M′ is the matrix obtained from M by replacing the ith column by the kth column, then detM is transformed into detM + c detM′. Thus a common factor of the values detM, when detM runs over all the minors of degree q, remains a common factor of them after any column-addition; the corresponding invariance holds for row-additions. By row-(column) multiplication, the minors take a unitfactor only. Hence, if $A \sim A'$, the highest common factor δ_q of the minors of degree q of A is a common factor of the minors of degree q of A′, but since also the converse holds, δ_q (which is determined up-to a unity-factor only) remains invariant. This holds for $q = 1, \ldots, n$ and $\delta_n = \det A$.

Let $b_1, \ldots, b_q$ be the elements of any row of M, and $B_1, \ldots, B_q$ their cofactors. Since

$$\det M = b_1 B_1 + \ldots + b_q B_q$$

holds, and the B's are divisible by δ_{q-1}, so detM is divisible by δ_{q-1}. This holds for every minor detM of degree q; hence δ_q is divisible by δ_{q-1}. The elements

$$\delta_1, \delta_2, \ldots, \delta_n \tag{3}$$

are called the *determinant divisors* of A. Using this notation, the results obtained here read as follows:

Theorem. Congruent matrices have the same system (3) of determinant divisors. For $i < k$, δ_i is a factor of δ_k.

This theorem applies also to the case when the Euclidean domain is a field, but then every element is either a unity or zero. Whithout loss of generality, one can assume that the determinant divisors are 1 or 0; if any one of the elements of the sequence (3) is 0, then the following elements are also equal to 0. The number of the elements equal to 1, is equal to rank (A). Thus the sequence (3) appears to be a generalisation of the notion of rank.

6·42. *"Sweep out" for matrices of* $R(\Delta, n)$. The determination of the determinant divisors is much simplified when the matrix is a diagonal-matrix. It has been shown in (1·4) how a matrix can be transformed by row-additions and permutations of columns into a diagonal-matrix, but in those investigations, the matrices were supposed to be matrices over a field, and the division by a matrix-element is indeed an important step when a matrix of that kind is swept out. To be applied to matrices of $R(\Delta, n)$, the method has to be modified; the operation of division will be replaced by the algorithmus of the *h. c. f.*, on the other hand one is allowed to make full use of the addition of columns. Whereas the considerations of 6·41 hold for every integral domain with unique factorisation, it is essential for the present section that Δ is a Euclidean domain.

Suppose $a^k_1 = a$ is the *h. c. f.* of the elements of the kth row of a matrix A, say $a^k_i = a\, a_i$ for $i = 2, \ldots, n$, then one can "sweep out" the row by the $n - 1$ column-additions $\alpha_i \rightarrow \alpha_i - a_i\, \alpha_1$; thereafter the kth row will be $(a, 0, \ldots, 0)$. If a^k_1 is not the *h. c. f.* of the kth row, but $a^k_j = a$ is, then $a^k_1 = a(a' + 1)$; by $\alpha_1 \rightarrow \alpha_1 - a\, \alpha_j$ the element a is brought to the first place in the row, and one can sweep out the row. The corresponding holds for columns. Thus if any element a^μ_ν of the matrix is equal to the invariant highest common factor δ_1, one can sweep out successively the

μ^{th} row, the first column, and then the first row without changing the first column. Thus the matrix is tranformed by row-and column-additions into

$$\begin{pmatrix} \delta_1 & \\ & A' \end{pmatrix}. \tag{1}$$

Suppose now that no element of A is equal to δ_1, (up to a unity factor). Since Δ is a Euclidean domain, a norm-function (see 2·4) for every element exists, and from the supposition follows that $N(a^\mu_\nu) > N(\delta_1)$. Let $a^i_k = a$ be an element of the matrix with the smallest occuring norm; it will be shown now that one can arrange by row-and column-additions that an element with a norm $< N(a)$ appears. Suppose that a is not the *h. c. f.* of the i^{th} row, say a^i_j is not divisible by a, then there exists an element

$$b = a^i_j - ca, \tag{2}$$

such that $N(b) < N(a)$. The column-addition $\alpha_j \to \alpha_j - c\,\alpha_k$ transforms a^i_j into b; correspondingly if there is an element in the k^{th} column which is non-divisible by a. If however every element of the i^{th} row is divisible by a, then sweep out the row; if thereafter in the first column there is an element which is non-divisible by a, one can apply the method given just before to replace this element by another with a norm $< N(a)$. If the elements of the first column are all divisible by a, then there must be elsewhere such an element, since a is not an *h. c. f.*; let a^μ_ν be such an element then $\mu \neq i$, $\nu \neq 1$; now $\alpha_1 \to \alpha_1 + \alpha_\nu$ leaves $a^i_1 = a$ unchanged and transforms $a^\mu_1 \to a^\mu_1 + a^\mu_\nu$ which is not divisible by a (since the first term is divisible and the second is not). Thus it is always possible to bring the element a in the same row or column with an element non-divisible by a and then to replace the latter one by an element b for which $N(b) < N(a)$. This method can be repeated untill (after at most $N(a) - N(\delta_1)$ steps) an element appears the norm of which is $N(\delta_1)$, and which is therefore an *h.c.f.* of the elements of A. By sweeping out, one gets hereafter A transformed into (1). Hence

Lemma. Every matrix A of $R(\Delta, \text{n})$ can be transformed by row-and column-additions into

$$\begin{pmatrix} \epsilon_1 & \\ & A' \end{pmatrix}, \tag{1'}$$

where $\epsilon_1 = \delta_1$.

Now A' can be transformed correspondingly by row and column-additions amongst the 2^{nd} to n^{th} rows (columns). By these operations the first row and the first column are unaltered. Thus one gets

$$A \simeq \begin{pmatrix} \varepsilon_1 & & \\ & \varepsilon_2 & \\ & & A'' \end{pmatrix}$$

where ε_2 is divisible by ε_1, and on the other hand ε_2 is an *h. c. f.* of the elements of A'. Thus after n steps one gets

$$A \simeq \begin{Vmatrix} \varepsilon_1 & & & & \\ & \cdot & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \varepsilon_n \end{Vmatrix} \tag{2}$$

where ε_{i+1} is divisible by ε_i.

Theorem. Every matrix A is congruent to a diagonal-matrix (2) where ε_{i+1} is divisible by ε_i, for $i = 1, \ldots, n-1$, and the congruence can be generated by row and column-additions. The elements ε_i are uniquely determined up to unity factors, and

$$\delta_q = \varepsilon_1 \ldots \varepsilon_q, \quad \text{for } q = 1, \ldots, n. \tag{3}$$

Proof. The first statement of the theorem has been proved already. The minors of any degree q of A are either equal to 0 or equal to products of diagonal elements $\pm\, \varepsilon_{1+t_1} \ldots \varepsilon_{q+t_q}$ where the t's are non-negative. Now ε_{i+t_i} is divisible by ε_i. Hence each of these determinants is divisible by $\varepsilon_1 \ldots \varepsilon_q$, and since the minor which is situated in the left upper corner is equal to that product, formula (3) holds. A unity factor remains arbitrary for each δ_q ; from (3) follows that

$$\varepsilon_q = \delta_q : \delta_{q-1}. \tag{3'}$$

Thus the ε's are determined up to a unity factor. This factor can be chosen arbitrarily, because a multiplication of the rows of (2) with unity elements is a congruence. Hence the theorem.

The elements $\varepsilon_1, \ldots, \varepsilon_n$ are called the *elementary divisors** of A, and (2) is the *canonical form* of A.

---

* The notation is not uniform ; some authors give this name to the factors $\varepsilon_i : \varepsilon_{i-1}$

Corollary. If in a diagonal-matrix D of $R(\Delta, n)$, every element is divisible by the preceding one, then D is a canonical form.

This corollary follows immediately from the uniqueness stated in the theorem.

Let $\alpha, \beta, \ldots, \mu$ be m elements of Δ which are relatively prime to one another; then the following matrices have the same elementary divisors as the canonical forms given below them:

$$\begin{matrix} \begin{pmatrix} \alpha^q & 0 \\ 1 & \alpha \end{pmatrix} & \begin{pmatrix} \alpha & \\ & \beta \end{pmatrix} & \begin{pmatrix} \alpha^p & \\ & \alpha^q \end{pmatrix} & \\ \begin{pmatrix} 1 & 0 \\ 0 & \alpha^{q+1} \end{pmatrix} & \begin{pmatrix} 1 & \\ & \alpha\beta \end{pmatrix} & \begin{pmatrix} \alpha^q & \\ & \alpha^p \end{pmatrix} & \text{(for } p > q). \end{matrix} \tag{4}$$

The alteration leading from the upper to the lower line can therefore be performed by row-(column-) addition and multiplication with a unity. This shows that by these operations a matrix of degree r

$$A_r = \left|\begin{matrix} \alpha & & & & \\ 1 & \cdot & & & \\ & \cdot & \cdot & & \\ & & \cdot & \cdot & \\ & & & 1 & \alpha \end{matrix}\right\| \text{ can be transformed into } \overset{0}{A}_r = \left\|\begin{matrix} 1 & & & \\ & \cdot & & \\ & & 1 & \\ & & & \alpha^r \end{matrix}\right\|$$

which is a canonical form. Moreover

$$A_{r_1, \ldots, r_p} = \begin{pmatrix} A_{r_1} & & & \\ & \cdot & & \\ & & \cdot & \\ & & & A_{r_p} \end{pmatrix} \simeq \begin{pmatrix} \overset{0}{A}_{r_1} & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \overset{0}{A}_{r_p} \end{pmatrix}$$

and from the last pair in (4) it follows that when $r_1 > r_2 > \ldots > r_p$,

$$A_{r_1, \ldots, r_p} \simeq \left\|\begin{matrix} 1 & & & & & & \\ & \cdot & & & & & \\ & & \cdot & & & & \\ & & & 1 & & & \\ & & & & \alpha^{r_p} & & \\ & & & & & \cdot & \\ & & & & & & \cdot \\ & & & & & & & \alpha^{r_1} \end{matrix}\right\| = \overset{0}{A}_{r_1, \ldots, r_p}$$

which again is a canonical form ; $\Sigma r_i = r$ is equal to the degree of the matrix. Form now such matrices for the m different elements $\alpha, \beta, \ldots, \mu$ and put them together to a matrix of degree $\Sigma r^j = n$, where $r^j = \sum_i r^j_i$, for $j = 1, \ldots, m$ and $r^j_1 > r^j_2 > \ldots > r^j_{p_j}$.

$$A = \left\| \begin{matrix} A_{r^1_1, \ldots, r^1_{p_1}} & & & \\ & B_{r^2_1, \ldots, r^2_{p_1}} & & \\ & & \ddots & \\ & & & M_{r^m_1, \ldots, r^m_{p_m}} \end{matrix} \right\| .$$

One can replace the matrices in the diagonal by their canonical forms, and then use the second pair of matrices in (4), then one gets

$$A^0 = \begin{pmatrix} \varphi_n & & \\ & \ddots & \\ & & \varphi_1 \end{pmatrix}, \text{ where}$$

$\varphi_i = \alpha^{r^1_i} \beta^{r^2_i} \ldots \mu^{r^m_i}$ and $r^j_i = 0$ if $i > p_j$. Again, this form is a canonical form. This example is important for 6-44.

6-43. *Congruence by matrix multiplication.* It has been shown in 1-(11)12 that row and column-additions can be performed by multiplication with certain elementary matrices $E_{r,s}(\lambda)$, where $\det E_{r,s}(\lambda) = 1$, and similarly row and column-multiplications, by multiplication with diagonal-matrices composed of the multipliers ; the multiplication with unities is therefore made by diagonal-matrices of unities. The determinants of these matrices are unities, and the same holds therefore for their products. Hence $A \sim B$ implies $B = U_1 A U_2$, where $\det U_1$, and $\det U_2$ are unities. It will be shown now that this condition for congruence is also sufficient. Since A can be transformed by row and column-additions into a diagonal-matrix, $A = \prod_1 D \prod_2$, where $\prod_1$ and $\prod_2$ are products of elementary matrices, and D is the canonical form of A. Since $\det \prod_1 = \det \prod_2 = 1$, so is $\det A = \det D = \prod_i \epsilon_i$. In the particular case when $A = U$, where $\det U$ is a unity, $\prod_i \epsilon_i$ is a unity and therefore each elementary divisor ϵ_i

is a unity. Hence U is a product of elementary matrices and a diagonal-matrix of unities. Let now $\det U_1$ and $\det U_2$ be unities and $B = U_1 A U_2$, then B is generated by multiplying A from both sides with elementary matrices and diagonal-matrices of unities; hence one can obtain B by performing row and column-additions and row and column-multiplications with unities. Thus A and B are congruent, and the following theorem holds.

Theorem. $A \sim B$, if and only if

$$B = U_1 A U_2, \tag{1}$$

where the determinants of U_1 and U_2 are unities.

If $\det U = u$ is a unity, then there exists in $R(\Delta, n)$ a matrix U^{-1} and $\det(U^{-1}) = u^{-1}$; thus $U_1^{-1} B U_2^{-1} = A$ is an equation of the same type as (1).

6-44. *The ring* $R(K[x], n)$. The ring of polynomials $K[x]$ over the field K is a Euclidean domain; its unities are the polynomials of degree 0, that is the elements of K which are different from *0* (see 2-47). Thus one can apply the theory of the elementary divisors to the matrices over $K[x]$, and the theorems of 6-42 and 6-43 furnish immediately:

Theorem 1. Every matrix B of $R(K[x]\ n,)$ can be represented by

$$B = B_1 \begin{Vmatrix} \varepsilon_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \varepsilon_n \end{Vmatrix} B_2, \tag{1}$$

where the determinants of B_1 and B_2 are elements $\neq 0$ of K, and the elementary divisors $\varepsilon_1, \ldots, \varepsilon_n$ are polynomials of $K[x]$, each being a factor of the following polynomials. The elementary divisors are uniquely determined up to factors which are elements $\neq 0$ of K and which can be chosen arbitrarily. The products $\varepsilon_1 \ldots \varepsilon_q = \delta_q$ are the determinant divisors.

Let Λ be an extension of K; then every matrix B over $K[x]$ is also a matrix over $\Lambda[x]$, and it admits also a representation by elementary divisors. Every *h.c.f.* of polynomials of $K[x]$ is also an *h.c.f.* of the same polynomials in $\Lambda[x]$, but for the *h.c.f.* in $\Lambda[x]$ the arbitrary factor is an element $\neq 0$ of Λ, whereas in $K[x]$, only a factor $\neq 0$ of K is arbitrary. Hence the determinant divisors $\delta_1, \ldots, \delta_n$ are the same in both the cases, up to a factor out of Λ which is arbitrary. If one multiplies a polynomial of $K[x]$ with an element of Λ which does not belong to K, then all the coefficients $\neq 0$ of the products are elements of Λ not belonging to K. Hence if δ_q is a determinant divisor of B which has been obtained by considering B as a matrix over $\Lambda[x]$, and if one of the coefficients $\neq 0$ of δ_q belongs to K, then δ_q is a polynomial of $K[x]$, and therefore δ_q is also the q^{th} determinant divisor when B is considered as a matrix over $K[x]$. The same holds for the elementary divisors, as these are quotients of determinant divisors. Hence :

Theorem 2. Let B be a matrix of $R(K[x], n)$ and $\Lambda \supset K$. If in $R(\Lambda[x], n)$,

$$B = \simeq \begin{pmatrix} \varepsilon_1 & & \\ & \ddots & \\ & & \varepsilon_n \end{pmatrix},$$

where $\varepsilon_1, \ldots, \varepsilon_n$ are polynomials in $\Lambda[x]$, with coefficients of the highest terms ± 1, and ε_i is a factor of ε_k in $\Lambda[x]$ for $i < k$, then $\varepsilon_1, \ldots, \varepsilon_n$ are polynomials in $K[x]$ and are the elementary divisors of B in $R(K[x], n)$.

This theorem will be applied now to

$$B = A - xE, \tag{2}$$

where A is a matrix over K. As in 6-33, denote by Λ an extension of K which contains all the roots of

$$\chi_A(x) = (\lambda_1 - x)^{r_1} (\lambda_2 - x)^{r_2} \ldots (\lambda_m - x)^{r_m}. \text{ Now}$$

$$A = C^{-1} \begin{pmatrix} L_1 & & \\ & \ddots & \\ & & L_m \end{pmatrix} C, \tag{3}$$

where C is a matrix over Λ, and $L_1, \ldots, L_m$ have the same significance as in 6-33, (8). Then

$$A - xE = C^{-1} \begin{Vmatrix} L_1 - xE_1 & & \\ & \ddots & \\ & & L_m - xE_m \end{Vmatrix} C,$$

where E_i is the unit-matrix of degree r_i. Since C is a matrix over Λ, it is a unity matrix of $R(\Lambda[x], n)$. In this ring, therefore

$$A - xE \simeq \begin{pmatrix} L_1 - xE_1 & & \\ & \ddots & \\ & & L_m - xE_m \end{pmatrix}.$$

Put $\lambda_1 - x = \alpha$, $\lambda_2 - x = \beta, \ldots, \lambda_m - x = \mu$, then these m elements of $\Lambda[x]$ are relatively prime to one another. One can therefore use the notations introduced at the end of 6-42, and one obtains the result

$$A - xE \simeq A^0 = \begin{pmatrix} \phi_n & & \\ & \ddots & \\ & & \phi_1 \end{pmatrix}. \tag{4}$$

where $\phi_i = \alpha^{r^1_i} \beta^{r^2_i} \ldots \mu^{r^m_i} = \phi_i(x)$.

$\phi_i(x)$ has the same meaning here as in (6-35,13). The polynomials $\phi_i(x)$ are therefore the elementary divisors of $A - xE$; the coefficients of the highest terms are ± 1. Hence:

Theorem 3. If A is a matrix over K, then the polynomials $\phi_i(x)$ of 6-35,(3) are the elementary divisors of $A - xE$ and are polynomials over K.

This theorem supplements the considerations of 6-33, 6-34 and 6-35. The canonical form A (see 6-34) determines uniquely the representation of the characteristic polynomial $\chi_A(x)$ as a product of polynomials $\phi_k(x)$ (see 6-35,(3), (4) and (5)). These polynomials have been introduced as polynomials in $\Lambda[x]$, where Λ is an extension of K admitting the complete reduction of $\chi_A(x)$. Now it has been shown that the polynomials belong to $K[x]$. On the other hand, the degrees r^i_k of the submatrices H^i_k of the canonical form of A are equal to the multiplicities of the roots of the polynomials $\phi_k(x)$. Thus the elementary divisors of $A - xE$ determine uniquely the canonical form of A up to an isomorphism of the field Λ over K.

6-45*. *The ring* $R(J, n)$. The integral numbers form a Euclidean domain J; its unities are $+1$ and -1. From 6-43 it follows therefore that every matrix C with integral elements can be written in the form

$$C = E_1 D E_2, \tag{1}$$

---

* Can be omitted at the 1st reading

where $\det E_1 = \pm 1$, $\det E_2 = \pm 1$, and D is a canonical form of C. Let D′ and D″ be diagonal-matrices with diagonal-elements ± 1 only, then $D'^2 = D''^2 = E$. In particular one can easily choose these matrices in such a manner that $\det E_1 D' = \det D'' E_2 = 1$, and that the elements of $D'DD''$ are either all positive, or the first is negative and the others are positive. Since $C = E_1 D', D'DD'', D''E_2$, there is no loss of generality in supposing that in (1),

$$\det E_1 = \det E_2 = 1, \quad D = \begin{pmatrix} \varepsilon_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \varepsilon_n \end{pmatrix}, \tag{2}$$

where for $i = 1, 2, \ldots, n$, $\varepsilon_i \geqq 0$, ε_i is divisible by ε_{i-1}. Put $E_2 E_1 = E'$, then

$$C \sim E_1^{-1}\, C\, E_1 = DE', \quad \det E' = 1. \tag{3}$$

Applying the transformations corresponding to the matrices of $R(J, \mathrm{n})$ to any given vector ξ of an n-dimensional Euclidean vectorspace, one obtains a modul

$$a_1\, \xi_1 + \ldots + a_n\, \xi_n, \tag{4}$$

where $a_1, \ldots, a_n$ run over all the integral numbers. The endpoints of these vectors form an n-dimensional *lattice* L. Every matrix C of $R(J, \mathrm{n})$ maps L on itself, but the mapping is not a (1, 1)-representation unless $\det C = \pm 1$. Similar matrices represent the same transformation for different bases. Hence by (3), every linear transformation of a lattice can be composed of a transformation E′ of the lattice into itself and a transformation D. To every basis of a sublattice S there corresponds a particular "mesh" which is "spun out" by the vectors of the basis; S is generated by parallel displacements of the mesh. On the other hand to every mesh there corresponds a sublattice S, and there exist linear transformations such that S is the image of L. By E′, the mesh spun out by the original basis of L is transformed into another mesh corresponding to L and by D this mesh is transformed into a mesh corresponding to the lattice S which is the image of L for the transformation C. Hence the theory of elementary divisors shows that if S is any sublattice of L, then there exist meshes M_1 and M_2 corresponding to S and L respectively, and one gets M_2 by multiplying the edges of M_1 with $\varepsilon_1, \ldots, \varepsilon_n$ respectively. Since these numbers are elementary divisors, each of them is a factor of the following ones.

6·5. *Matrices and forms.*

A column-vector (x), when multiplied from the left side with an arbitrary matrix, is transformed again into a column-vector $A(x) = (x)$. Similarly a row-vector $(x)^T$ is transformed into a row-vector by multiplication from the right side. Thus a product of matrices

$$(x)^T \; A(y) \tag{1}$$

is a matrix of which every element is necessarily equal to zero except the first element in the first row, and this can easily be stated to be equal to

$$f(x, y) = \Sigma \, a^i_k \; x_i \; y_k. \tag{2}$$

Every *bilinear form* in x and y can be written in the form (2). Hence one can apply the theory of matrices to bilinear forms. E.g. the transformation of the bilinear forms can easily be expressed by matrices. Suppose $(x) = B(u)$, $(y) = C(v)$, then $(x)^T = (u)^T \, (B)^T$, and $(x)^T A(y) = (u)^T \, B^T \, AC(v)$. Put

$$G = B^T \; A \; C, \tag{3}$$

then

$$f(x, y) = \Sigma \; g^\mu{}_\nu \; u_\mu \; v_\nu. \tag{4}$$

Let in particular, (x) and (y) be the expressions for two vectors of a vectorspace when a particular basis is used, and let (u) and (v) be the same vectors expressed by a different basis, then $B = C$, and therefore

$$G = B^T \; A \; B. \tag{3'}$$

This case is of particular interest; for instance it occurs when $(x) = (y)$. Thus the linear transformation of a *quadratic form*

$$f(x, x) = \Sigma \, a^i_k \; x_i \; x_k \rightarrow g^\mu{}_\nu \; u_\mu \; u_\nu = g(u, u) \tag{5}$$

can be obtained by the help of (3'). The vectors (x) and (y) can also be interconnected in a different manner. E.g. the two vectors can be supposed to be conjugate (see 6·51), or it can be postulated that when the (x) vector is transformed, the (y) vectors are transformed in such a way that a certain bilinear form remains invariant.

6·51. *Unitary matrices.*

From 6·5,(3) it appears already, that the theory of similarity of matrices (see 6·3 and sub-sections) can be applied to the transformation of a quadratic form, when $B^T = B^{-1}$. Matrices with this property therefore promise to be particularly interesting. It is however preferable to use here a slight generalisation.

Consider two fields K and Λ ; as in 2-742 and in 3-33, it is supposed that $[\Lambda : K] = 2$ and that therefore Λ consists of pairs of conjugate elements. For these pairs, *the same suppositions are made here, as in* 3-33, and therefore the theorems established there can be applied here. It is convenient to introduce the notation M for a field

$$\begin{aligned} &\text{either } M = K, \\ &\text{or } \quad\;\; = \Lambda \end{aligned} \tag{1}$$

to avoid repetition of the same considerations. If $M = K$, conjugate elements are equal, $\bar{\alpha} = \alpha$, and $\bar{\alpha}\,\alpha = \alpha^2$; if $M = \Lambda$, a distinction between conjugate elements must be made. The most important case for applications is, when Λ is the field of the complex numbers and K the field of the real numbers. The conditions of 3-33 are obviously satisfied for this pair of fields.

Let $(a^i_k) = A$, then denote

$$(\bar{a}^i_k) = \bar{A}. \tag{2}$$

Since the interchange of conjugate elements is an automorphism (in the case when $M = K$, it is even the identity), for every polynomial $f(x)$ of $M[x]$,

$$f(\bar{A}) = \overline{f(A)}. \tag{3}$$

In particular $\bar{A}^{-1} = \overline{A^{-1}}$. Moreover the conjugate matrix to the transposed is the transposed of the conjugate, and $\overline{\det A} = \det \bar{A}$. Denote

$$\bar{A}^T = A^T = A^+. \tag{4}$$

Obviously $(\bar{A}^T)^T = (\bar{A}) = (A^+)^+ = A$, and from (4) it follows that $(A^T)^+ = (A^+)^T$, and $(\bar{A})^+ = \overline{A^+}$. The elements of A^{-1} are $A^i_k : \det A$, and since $\det A^T = \det A$, and the elements of $(A^T)^{-1}$ are $A_i^k : \det A$. Hence $(A^T)^{-1} = (A^{-1})^T$ and — taking the conjugate — $(A^+)^{-1} = (A^{-1})^+$. All these statements are comprehended in the following lemma.

Lemma. The symbols T, +, —, — 1 as exponents of a matrix are commutative.

Apply these symbols to a product of two matrices, and record :

$$\overline{A\,B} = \bar{A}\,B \tag{5}$$

$$(AB)^T = B^T A^T,\ (AB)^{-1} = B^{-1} A^{-1},\ (AB)^+ = B^+ A^+.$$

Definition. U is said to be a *unitary* matrix over M if

$$U^{*} = U^{-1}. \tag{6}$$

Let U, U_1, U_2 be unitary matrices of degree n over M. Then U^{-1} and $U_1\,U_2$ are unitary; indeed $(U^{-1})^{*} = U^{**} = U = (U^{-1})^{-1}$, and $(U_1\,U_2)^{*} = U_2^{*}\,U_1^{*} = U_2^{-1}\,U_1^{-1} = (U_1\,U_2)^{-1}$. In particular, the matrix $E = E^{*} = E^{-1}$ is a unitary matrix. (This shows that unitary matrices really exist). Hence the unitary matrices of degree n over M form a system

$$G_u(n, M) \tag{7}$$

with the following properties:

1. There exists an associative composition of the matrices, such that if U_1 and U_2 belong to (7), then also $U_1\,U_2$ belongs to it.

2. $G_u(n, M)$ contains a unit-element E, such that $UE = EU = U$ holds for every element U of it.

3. To every U of $G_u(n, M)$, there corresponds an inverse element U^{-1} in $G_u(n, M)$ satisfying $U\,U^{-1} = U^{-1}\,U = E$.

Apply the notation already introduced in 6·1f, and express these statements by:

Theorem 1. The matrices of $G_u(n, M)$ form a group. (The group of the unitary matrices of degree n over M).

From the lemma and (6) it follows immediately that when U belongs to $G_u(n, M)$, then, besides U^{-1}, also U, U^{T} and U^{*} belong to it. Moreover the "norm"

$$\det U\,(\overline{\det U}) = 1 \tag{8}$$

for every unitary matrix, since $\overline{\det U} = \det \overline{U} = \det U^{*} = \det(U^{-1}) = (\det U)^{-1}$.

Express (6) in terms of elements u^{i}_{k}. Put $U\,U^{*} = C$. Then

$$c^{i}_{k} = \sum_{j} u^{i}_{j}\ u^{k}_{j},\ \overline{u}^{k}_{j}$$

and since (6) means that $C = E$, one gets

$$\begin{aligned} \Sigma\, u^{i}_{j}\ \overline{u}^{k}_{j} &= 0 \quad \text{for } i \neq k \\ &= 1 \quad \text{for } i = k \end{aligned} \tag{6'}$$

as a system of equations which is equivalent to (6). Since U^T is also unitary,

$$u^j{}_i\,\bar{u}^j{}_k = 0 \quad \text{for } i \neq k \tag{6''}$$
$$= 1 \quad \text{for } i = k.$$

On the other hand, if U^T is unitary, then U is. Hence (6″) implies (6′). Hence (6), (6′) and (6″) are equivalent systems of necessary and sufficient conditions for the unitariness of U. A fourth form for these conditions is

$$u^{-1}{}_k = U^k{}_i : \det U. \tag{6'''}$$

It has already been mentioned that E is a unitary matrix, but it has not yet been proved that there exist unitary matrices which are not unit matrices. As a matter of fact, one can choose the first row of a unitary matrix nearly arbitrarily. It has been proved already in 3-33,th.2 that given any system $v_1, \ldots, v_n \neq 0, \ldots, 0$ of elements of M, one can find n^2 elements $u^i{}_k$ satisfying (6′) such that $u^1{}_k = \lambda\, v_k (k = 1, \ldots, n)$; obviously one can determine the $u^i{}_k$ also in such a way that $u^k{}_1 = \lambda\, v_k$. In terms of matrices this means :

Theorem 2. Let $v_1, \ldots, v_n$ be n elements of M but different from $0, \ldots, 0$, then there exists a unitary matrix, the first row (column) of which differs from $v_1, \ldots, v_n$ by a factor λ only which is a suitably chosen element of M.

It may be remembered that in 3-33, the factor λ was determined by the condition $N(\lambda) = \Sigma\, v_j\, \bar{v}_j$. Therefore λ can be replaced by $\alpha\,\lambda$, where α is any element with $\alpha\,\bar{\alpha} = 1$. In particular λ can always be replaced by $-\lambda$.

If U and U_1 are unitary, then

$$\begin{pmatrix} U & \\ & U_1 \end{pmatrix} \tag{9}$$

satisfies the conditions (6′) and is therefore unitary. In particular $\begin{pmatrix} E & \\ & U \end{pmatrix}$ is unitary.

Consider now a vectorspace, say V of rank n over M, and distinguish in it a basis

$$\varepsilon_1, \ldots, \varepsilon_n. \tag{10}$$

Let U be a unitary matrix of degree n over M and **U** be the transformation of V which one gets by applying U to the basis (10). Since there exists an inverse transformation of $\mathbf{U}$, the basis (10) is transformed by $\mathbf{U}$ into n independent vectors

$$\varepsilon'_1, \ldots, \varepsilon'_n \tag{10'}$$

which form a basis of V expressed in terms of the basis (10).

$$\varepsilon'_k = (u^1_k, \ldots, u^n_k),$$

i.e. the vectors (10′) are expressed by the columns of the unitary matrix U. Let U run over all the matrices of $G_u(\mathrm{n}, \mathrm{M})$ then (10′) runs over all the systems of n vectors for which the scalar products satisfy the conditions

$$\varepsilon'_i \overline{\varepsilon'_i} = 1, \quad \varepsilon'_i \overline{\varepsilon'_k} = 0, \text{ for } \mathrm{i} \neq \mathrm{k}. \tag{11}$$

Thus given any basis (10), the group $G_u(\mathrm{n}, \mathrm{M})$ generates a system Σ of bases of V, the coordinates of which (expressed by (10)) satisfy the conditions (11). Let (10) be transformed into (10′) by $\mathbf{U}$ and into $\varepsilon''_1, \ldots, \varepsilon''_n$ by $\mathbf{U}$, then $\mathbf{U}_1 \mathbf{U}^{-1}$ transforms ε'_k to ε''_k. Now $\mathrm{U}_1 \mathrm{U}^{-1}$ is a unitary matrix; hence if one applies the unitary matrices to any basis of the system Σ, one gets the same system Σ of bases. A transformation of V which is obtained by applying a unitary matrix to a particular basis of the system Σ is called a *unitary transformation*. It must be emphasised that for unitary transformations the bases of V are not all equivalent, but particular systems of bases are distinguished. Let $\beta_1, \ldots, \beta_n$ be an arbitrary basis (see 6-2) and $\beta_k = \sum\limits_i b^i_k \varepsilon_i$, then the unitary transformations of V are expressed by the β-basis by the matrices

$$\mathrm{B}^{-1}\, \mathrm{U}\, \mathrm{B},$$

and these matrices are in general not unitary. On the other hand a transformation which is represented by a unitary matrix when the β-basis is used, might be expressed by a non-unitary matrix when the original basis is used, and therefore it will not be a unitary transformation.

6-511. *Orthogonal matrices.* Consider now the particular case when $\mathrm{M} = \mathrm{K}$. Then $\mathrm{A} = \bar{\mathrm{A}}$, $\mathrm{A}^T = \mathrm{A}^*$. Unitary matrices are called *orthogonal* in this case. From 6-51, (6), (6′), (6″) and (8) it follows that if R is an orthogonal matrix, the following equations hold:

$$\mathrm{R}^T = \mathrm{R}^{-1}, \quad \sum_k r^i_k r^j_k = \sum_k r^k_i r^k_j = 0 \text{ for } \mathrm{i} \neq \mathrm{j}$$

$$\det\mathrm{R} = \pm 1, \; \sum_k (r^i_k)^2 = \sum_k (r^k_i)^2 = 1. \tag{1}$$

The n row-vectors, and the n column-vectors form therefore two "orthogonal systems" (see 1-7, Def. 3).

If in particular K is the field of the real numbers, then V is an n-dimensional Euclidean vector-space. Let in this space

$$\varepsilon_1, \ldots, \varepsilon_n \tag{2}$$

be n mutually perpendicular vectors of equal length, say length 1 ; then this basis is transformed by R into n mutually orthogonal vectors of length 1; these n-tuplets form the system of bases which in 6-51 was called Σ. The matrices of $G_u(n, K)$ represent the rigid motions of V if $\det R = 1$ and the symmetries if $\det R = -1$, when the basis (2) or an equivalent basis (*i.e.* a basis of Σ) is used. The rigid motions and symmetries of an n-dimensional Euclidean point-space are composed of the corresponding transformations of V and parallel displacements. Theorem 2 of 6-51 shows that the direction of one vector of an orthogonal system can be arbitrarily chosen.

6-52. *Symmetric and antisymmetric matrices.*

Definition 1. A matrix S is called *symmetric* if

$$S = S^T. \tag{1}$$

Definition 2. A matrix is called *antisymmetric* (or *skew*) if

$$A = -A^T. \tag{2}$$

These definitions are applied to matrices over arbitrary fields and integral domains. In terms of elements, a symmetric matrix S is characterised by

$$s^i{}_k = s^k{}_i. \tag{1'}$$

Antisymmetric matrices over a field of characteristic 2 are symmetric (and conversely) ; if the characteristic of K is *different* from 2, then an antisymmetric matrix is characterised by

$$\begin{aligned} a^i{}_k &= -a^k{}_i \\ a^i{}_i &= \quad 0. \end{aligned} \tag{2'}$$

Let B be an arbitrary matrix over a field K of characteristic $\neq 2$, then

$$B = S + A, \tag{3}$$

where $s^i{}_k = (b^i{}_k + b^k{}_i) : 2$, $a^i{}_k = (b^i{}_k - b^k{}_i) : 2$.

It is easy to see that the representation (3) of B is possible in this way only.

Exercises. (1). Every antisymmetric matrix of rank r is similar to a matrix $\begin{pmatrix} A & \\ & O \end{pmatrix}$, where A is antisymmetric and of degree r.

(2). The rank of an antisymmetric matrix is necessarily even.

(3). Let A be antisymmetric and of degree 2n, and let the $m = n(2n-1)$ elements of A above the diagonal be indeterminates $y_1, \ldots, y_m$; then $\det A = f^2(y_1, \ldots, y_m)$, where f is irreducible.

6-53. *Hermitean matrices.* Here again, the notations K, Λ, M are used as in 6-51.

Definition. A matrix N over M is said to be Hermitean over M if

$$H^* = H \tag{1}$$

and the roots of $\chi_H(x)$ belong to M. If U is unitary and H is Hermitean over M, then $H_1 = U^{-1}H\ U$ is also Hermitean over M. Of course it follows from (1) and from 6-51,(5) and (6) that $H^*_1 = U^*\ H^*(U^{-1})^* = H_1$, and $\chi_{H_1}(x) = \chi_H(x)$; hence the roots of this polynomial belong to M. For the elements h^i_k of H

$$h^i_k = \bar{h}^k_i \tag{2}$$

holds. In particular the diagonal elements $h^i_i = h^i_i$ are self-conjugate and therefore belong to K. If all the elements of H belong to K, then H is symmetric. If H_2 and H_3 are Hermitean, then

$$H_1 = \begin{pmatrix} H_2 & \\ & H_3 \end{pmatrix}$$

is Hermitean, and conversely. If in particular

$$H_1 = \begin{pmatrix} \lambda & \\ & H' \end{pmatrix} \tag{3}$$

is Hermitean, then λ belongs to K, and H′ is Hermitean. From this remark will be deduced the following

Theorem 1. If H is Hermitean over M, the roots of $\chi_H(x)$ belong to K.

Proof. Let λ be any root of $\chi_H(x)$, then λ belongs to M and there exists in the vectorspace V over M a vector $\xi = (v_1, \ldots, v_n)$ such that

$(H - \lambda E)\, \xi = O$. Let U_1 be a unitary matrix whose first column differs from $v_1, \ldots, v_n$ by a common factor only (see 6-51, th. 2), then

$$H_1 = U_1^{-1}\, H\, U_1 \tag{4}$$

transforms $(1, 0, \ldots, 0)$ into $(\lambda, 0, \ldots, 0)$ and this must be the first column of H_1. Since H_1 is Hermitean, the first row must be conjugate to the first column. Hence H_1 has the form (3) ; thus λ belongs to K. Hence the theorem.

Applying this theorem to matrices over K, one gets immediately :

Theorem 1′. If S is symmetric over K, and the roots of $\chi_s(x)$ belong to Λ then these roots belong to K.

Moreover :

Theorem 2. If H is Hermitean over M, then there exists a matrix U which is unitary over M such that

$$H = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} U^{-1}, \tag{5}$$

where $\lambda_1, \ldots, \lambda_n$ are the roots of the characteristic polynomial of H.

Proof. Let λ_1 be any root of $\chi_H(x)$, then it follows from (3) and (4) that $H = U_1\, H_1\, U_1^{-1}$, where $H_1 = \begin{pmatrix} \lambda_1 & \\ & H' \end{pmatrix}$. Let λ_2 be a root of H'. Since H' is a Hermitean matrix of degree $n - 1$, there is a Hermitean matrix $H'_1 = \begin{pmatrix} \lambda_2 & \\ & H'' \end{pmatrix} = U'^{-1}_1\, H'\, U'_1$, where H'' is Hermitean and U'_1 is unitary and of degree $n - 1$; hence $U_2 = \begin{pmatrix} 1 & \\ & U'_1 \end{pmatrix}$ is unitary and of degree n (see 6-51, (9)). From 6-13,(2) it follows that

$$H = U_2\, U_1 \begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & H'' \end{pmatrix} U_1^{-1}\, U_2^{-1}.$$

Repeat this step n times and put $U_n \ldots U_2\, U_1 = U$; then U is unitary and the theorem follows.

Put M = K, then the unitary matrix U is an orthogonal matrix. From theorem 1′ and theorem 2 it follows therefore immediately :

Theorem 2′. If S is a symmetric matrix over K and the roots of $\chi_S(x)$ belong to Λ, then

$$S = R \begin{pmatrix} \lambda_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \lambda_n \end{pmatrix} R^{-1}, \tag{6}$$

where R is an orthogonal matrix over K.

The condition that the roots of $\chi_S(x)$ belong to Λ can be omitted when Λ is known to be a closed field (see 3-8). Now the field of the complex numbers is a closed one, and the fields of the real and of the complex numbers form a pair of fields K, Λ satisfying the conditions of 6-51. Applied to this particular pair of fields, the theorems 1′ and 2′ furnish :

Theorem 3. If S is a symmetric matrix over the field of the real numbers, then the roots $\lambda_1, \ldots, \lambda_n$ of its characteristic polynomial are all real, and S can be transformed by an orthogonal transformation into the diagonal-matrix

$$\begin{pmatrix} \lambda_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \lambda_n \end{pmatrix} \tag{7}$$

The equation $\chi_S(x) = 0$ is often called *secular equation* on account of its importance for the theory of secular disturbances.

6·54. *Hermitean and quadratic forms.* Extend the field M to a ring of polynomials,

$$M[\{x\}] \tag{1}$$

by introducing 2n or n indeterminates. If M = Λ, there are 2n indeterminates

$$\begin{matrix} x_1, \ldots, x_n \\ \bar{x}_1, \ldots, \bar{x}_n. \end{matrix} \tag{2}$$

If M = K, there are n indeterminates $x_1, \ldots, x_n$ only, but one may use the notation (2), and put $\bar{x}_i = x_i$ for i = 1, …, n. In both cases, x_i and $\bar{x}_i$

are said to be *conjugate*. Thus one can extend the automorphism interchanging conjugate elements of M to an automorphism

$$\sum a_{s \cdots r,\, s' \cdots r'}\, x^{s}_{1} \ldots x^{r}_{n}\, \bar{x}^{s'}_{1} \ldots \bar{x}^{r'}_{n} \longleftrightarrow \sum \bar{a}_{s \cdots r,\, s' \cdots r'}\, \bar{x}^{s}_{1} \ldots \bar{x}^{r}_{n}\, x^{s'}_{1} \ldots x^{r'}_{n} \tag{3}$$

which interchanges conjugate elements of M as well as conjugate indeterminates (2). When M = K, then (3) is the identity. Let (x) be the column-vector with the elements $x_1, \ldots, x_n$, then $(x)^*$ is the row-vector with elements $\bar{x}_1, \ldots, \bar{x}_n$. If H is Hermitean over M,

$$F = (x)^*\ H\ (x) = F^* \tag{4}$$

is a matrix, the first element of which is equal to

$$f(\bar{x}, x) = \sum h^{i}_{k}\ \bar{x}_i\ x_k = \bar{f}(x, \bar{x}), \tag{5}$$

whereas the other elements are equal to 0. The bilinear form (5) is called a *Hermitean form*. In the particular case when M = K, the form is a *quadratic form*.

$$f(x, x) = \sum h^{i}_{k}\ x_i\ x_k = \sum h^{i}_{i}\ x^2_i + 2 \sum_{i<k} h^{i}_{k}\ x_i\ x_k. \tag{6}$$

On the other hand every quadratic form over a field of characteristic $\neq 2$ can be expressed by (6). The fields K, Λ, M are all supposed to be of characteristic 0 (see 3-33). The theorems of 6-53 furnish therefore:

Theorem 1. By a unitary transformation of $x_1, \ldots, x_n$ say $(x) \rightarrow U(x)$, $(x)^* \rightarrow (x)^*\ U^*$, every Hermitean form over Λ can be transformed into a canonical form over K

$$\sum a_i\ x_i\ \bar{x}_i. \tag{7}$$

Theorem 2. By an orthogonal transformation of $x_1, \ldots, x_n$ every quadratic form over K can be transformed into a canonical form

$$\sum a_i\ x^2_i. \tag{8}$$

A transformation of $x_1, \ldots, x_n$ by U means that the corresponding Hermitean matrix is transformed into a similar one. Now two similar diagonal-matrices have the same diagonal-elements (only they may be arranged in a different order). Hence the coefficients a_i in (7) and (8) are uniquely determined. They are the roots of the characteristic polynomial. In terms of forms, the unitary matrices are characterised as follows:

Theorem 3. A matrix U is unitary if and only if the form

$$\Sigma \bar{x}_i x_i \tag{9}$$

is invariant for the transformation $(x) \to \mathrm{U}(x)$, $(\bar{x})^T \to (x)^T \mathrm{U}^*$.

Proof. The Hermitean matrix corresponding to (9) is E, the matrix of the transformed Hermitean form is therefore $\mathrm{U}^* \mathrm{E} \mathrm{U}$. Now the two equations $\mathrm{U}^* \mathrm{EU} = \mathrm{E}$ and $\mathrm{U}^* = \mathrm{U}^{-1}$ are equivalent. The first equation means that (9) is invariant for U, the second equation is the condition for U being unitary. Hence the theorem.

6-541. *The law of inertia for quadratic forms with real coefficients.* Though there is one and only one canonical form

$$\Sigma a_i x_i^2 \tag{1}$$

in which a quadratic form over K can be transformed by orthogonal transformations, this canonical form might be simplified by non-orthogonal transformations. Indeed, put $x_i = b_i x'_i$, then (1) is transformed into $\Sigma a'_i x'^2_i$, where $a'_i = a_i b^2_i$. Hence the coefficients a_i take factors which are arbitrary squares in K. If in particular, K is chosen as the field of the real numbers, the b's can be selected in such a way that a'_i takes only the values $+1$, -1 and 0. That there is no further reduction of the canonical form, is shown by the following theorem.

Law of inertia for quadratic forms. Any quadratic form in $x_1, \ldots, x_n$ with real coefficients can be transformed by a matrix of rank n with real elements into one and only one canonical form

$$q(x) = x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_r^2 \tag{2}$$

where $\mathrm{p} \leqq \mathrm{r} \leqq \mathrm{n}$.

Proof. That a transformation of any form into (2) can be performed, has been shown already. The number r is equal to the rank of the matrix S which corresponds to (2), and it is also the rank of every matrix $\mathrm{A}^T \mathrm{S} \mathrm{A}$, when A is of rank n. Hence r is an invariant for the transformations under consideration. It remains to show that p is an invariant. Suppose

$$q_1(z) = z_1^2 + \ldots + z_q^2 - z_{q+1}^2 - \ldots - z_r^2 \tag{2'}$$

$x_i = b^i_1 z_1 + \ldots + b^i_r z_r$, $z_i = c^i_1 x_1 + \ldots + c^i_r x_r$, for $\mathrm{i} = 1, \ldots, \mathrm{r}$. Then $q(x) = q_1(z)$ for corresponding values of x and z. It has to be proved that $p = q$. Let $p \neq q$, say $p > q$ (without loss of generality), and solve the $q + r - p < r$ linear homogeneous equations :

$$c^k{}_1\, x_1 + \ldots + c^k{}_r\, x_r = 0 \text{ for } k = 1, \ldots, q$$

$$x_t = 0 \text{ for } t = p + 1, \ldots, r.$$

These equations have a solution $(\xi_1, \ldots, \xi_p, 0, \ldots, 0) \neq (0, \ldots, 0)$. In terms of z the equations (3) are expressed by

$$z_s = 0 \text{ for } s = 1, \ldots, q$$

$$b^j{}_1\, z_1 + \ldots + b^j{}_r\, z_r = 0 \text{ for } j = p + 1, \ldots, r.$$

The corresponding solution is $(0, \ldots, 0, \zeta_{q+1}, \ldots, \zeta_r)$. Now $q(\xi) > 0$, $q_1(\zeta) \leqq 0$, contrary to $q(\xi) = q_1(\zeta)$. Hence the theorem.

A quadratic form with real coefficients is called *positive definite* if in the canonical form (2), there is $n = r = p$; if however $n = r$, $p = 0$, it is said to be *negative definite* ; when $n > r$ and $p = r$ or 0, it is *semi-definite*, and when $r > p > 0$ it is *indefinite*.

6·542. *Applications to Geometry.* The theory of matrices and of quadratic forms admits a large number of applications to Geometry of which a few may be mentioned here. A linear transformation of $x_1, \ldots, x_n$ means a collineation of an $(n - 1)$-dimensional projective space when homogeneous coordinates are used, and it means an affinity with fixed origin of an n-dimensional space when non-homogeneous coordinates are used. An orthogonal transformation has to be interpreted as a rigid motion or a symmetry (according as the determinant is $+1$ or -1) of a metrical n-dimensional space the origin remaining fixed. If one multiplies any column of an orthogonal matrix with -1, it remains orthogonal, and its determinant changes sign. It is therefore possible to transform a quadratic form with real coefficients into the canonical form by an orthogonal transformation with deteminant $+1$. In a projective $(n - 1)$-dimensional space, an orthogonal transformation means a collineation for which the quadric $x^2{}_1 + \ldots + x^2{}_n = 0$ remains invariant. Forms occuring in Geometry are either completely determined, or they are only the left side of an equation where the right side is zero ; in the latter case, they are determined up to an arbitrary factor $\neq 0$ only. By these considerations, the preceding result furnishes easily the complete classification of the quadrics of an n-dimensional metric space as follows

$$\begin{array}{ll} 1. & a_1 x_1^2 + \dots + a_n x_n^2 + 1 = 0 \\ 2. & a_1 x_1^2 + \dots + a_{n-1} x_{n-1}^2 + x_n = 0 \\ 3. & a_1 x_1^2 + \dots + a_n x_n^2 = 0. \end{array} \qquad (1)$$

In the first case, the a's are uniquely determined, in the second, a factor ± 1 remains arbitrary and in the third case a real factor of the a's is undetermined.

For the affine space, there are also the canonical forms (1) but the a's are supposed to take the values $+1$, -1, 0 only. For the projective (n — 1)-dimensional space, the canonical forms are

$$x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_r^2 \qquad (2)$$

with $r/2 \leqq p \leqq r \leqq n$.

6-55. *Bilinear forms with contragradient indeterminates.* At the beginning of 6-5, it has been shown that a bilinear form $f(x, y) = \Sigma a^i_k x_i y_k$ can be represented by a matrix product $(x)^T A(y)$, and that the transformations $(x) = B(u)$, $(y) = C(v)$ generate a transformation

$$A \rightarrow B^T AC. \qquad (1)$$

This formula has been applied to cases when (x) and (y) are either identical or conjugate, but they may also be linked together in a different manner.

(1). The vectors (x) and (y) are bound to be transformed in the same way ; then they are said to be *cogradient*. In this case, $B = C$ and therefore

$$A \rightarrow B^T AB. \qquad (2)$$

A pair of points of an n-dimensional Euclidean space is an instance of two cogradient vectors, but for "point" one may take also any other geometrical entity expressed by coordinates.

(2). The vectors (x) and (y) are bound to be transformed in such a way that the bilinear form $x_1 y_1 + \dots + x_n y_n$ remains invariant. Then $B^T EC = E$, and therefore $B^T = C^{-1}$. Hence

$$(x) \rightarrow (C^T)^{-1} (x), \; (y) \rightarrow C(y), \quad A \rightarrow C^{-1} AC. \qquad (3)$$

In this cas the vectors (x) and (y) are said to be *contragradient*.

E.g. the points and the straight lines of a projective plane are contragradient. The distinction between cogradient and contragradient vectors is fundamental for *Tensoralgebra* which forms the basis of analytic and differential geometry.

INDEX

Abelian group 50
addition 49
— of matrices 243
— of polynomials 74
— in a quotientfield 67
— of vectors 13
additive language 56
algebraic extension 104
algorithmus of division 89
— of *h.c.f.* 86
antisymmetric matrix 293
approximation 201
— of positive numbers 176
— of quadratic numbers 179
— of roots of polynomials 202-236
— of square roots 183
— by rational functions 191
associates 81
associative law (see : law)
automorphism 57
— of a Galoisfield 125
— of a normal extension 116

Basis of a vectorspace 15,101
— — over K 105
block design 130
Brahmagupta 185
Budan-Fourier's theorem 218

Calculation in a Galoisfield 125
— of periodic continued fractions 179
(see also : approximation)
canonical form of a matrix 273; 281
Cauchy, A.L. 130
changes of sign 213
—, alterations of 214
characteristic 64
— polynomial (equation) 260
— —, multiple roots of 262
classes of residues 51
classical algebra 160
closed field 158
coefficient 73
cofactor 32
—, generalised 38
cogradient 300
column 17
— vector 77, 250
commutative (see : group, law ring)
composition of permutations 4
— of transformations 44
congruent matrices 277
— numbers 51
conjugate elements 117
— indeterminates 297
— matrices 289
continued fraction 161
—, complete 164
—, convergence of 194
—, convergent of 164
—, finite (infinite) 162
—, periodic 176
— —, calculation of 179
— —, purely 178
—, representation of elements of B by 189
—, — of numbers by 170
— with polynomials as elements 191
— with rational elements 193
contragradient 300
coordinates of an *n*-vector 13

Decomposition of matrices 46
— of permutations 5
definite quadratic form 299
degree of an element over K 104
— of a matrix 242
— of a polynomial 73
— of a series $\phi(x)$ 187
dependent vectors 14,103
derivative 78
Descartes' rule 219
determinant 29
— divisor 279
—, irreducibility of 141
diagonal-matrix 46
discriminant 212
distributive (see : law)
division (see : algorithmus)
domain of the integral numbers 87
— with factorisable elements 82
—, Euclidean 85
—, integral 68

Eisenstein's theorem 138
element 50
—, conjugate 117
—, degree of 104
—, prime- 81
—, singular 53
elementary divisor 281
— matrix 46
elliptic substitution 274
equation, binomial 148
—, biquadratic 151
—, characteristic 260
—, cubic 149
—, secular 296
(see also : linear)
equivalence 51
—, (im-)proper 168
Euclidean domain 85
Euler's formula 80
even number 1
— permutation 6
exponent of vector 267
extension of a field 95
— — , algebraic 104

— — , finite 103
— — , normal 113
— — , primitive element of 110
— — , repeated 109
— — , smallest 114
— — , transcendental 104
— — and *h.c.f.* 106
— — by roots of two polynomials 112
— of a Galoisfield 123
— of an isomorphism 113
— of a ring of polynomials 78
extrapolation 241

Factor 80
—, highest common 84
(see also : extension)
factorisable 81
factorisation 80
— in $D[x]$ 91
— in $F[x]$ 88
— into linear factors 98
— , unique 81
—, — , criterion of 83
Fermat 185
— theorem 127
field 56
— $K(i)$ 130
— $R(i)$ 131
— , characteristic of 64
— , closed 158
— , nulielement of 57
— rank of a vectorspace (field) over 101(105)
— , singular element of 56
— , unitelement of 57
— , vectorspace over 100
(see : extension, Galoisfield, primefield, quotientfield, subfield)
finite continued fraction 162
— extension 103
— geometry 128
— over K 104
fixpoint 247
form = homogeneous polynomial 79
— , bilinear 288
— , Hermitean 297
— , quadratic 288
—, — , (in-)definite 289
— applied to geometry 299
function 202
— of a column-vector 30
— of a matrix 29
— , bilinear 38
— , integral 76
— , norm- 86
— , symmetric rational 147
functional manner of notation 4
fundamental theorem of classical algebra 160
— — of general algebra 95

Galoisfield 121
—, application to finite geometry 128
—,— to statistical analysis 129
—,— to theory of numbers 127
— , automorphism of 124
— , calculation in 125
— , finite extension of 123
— , primitive element of 123
Gauss' theorem 237
Graeffe's method 229
group 246
— , abelian 50
— , commutative 247
— of matrices 247

Hermitean form 297
— matrix 294
highest common factor = *h.c.f.*
(see : factor)
height of a vector 241
homogeneous linear equations 20
— polynomials 79
homomorphism 57
— mod. a prime-element 88
— , proof of irreducibility by 138
— , ring generated by 59
Horner's scheme 202
hyperbolic substitution 274

Identification 69
image 58
indefinite quadratic form 299
independent vectors 15
indeterminate 73
— , conjugate 297
induction, mathematical 2
integral domain 68
— — , unity of 80
— function 76
— number 87
interpolation 238
— , linear 226
inverse of a linear transformation 47
— of a matrix 48
(see also : law)
irrationality 195
irreducibility 135
— of cyclotomic polynomials 139
— of determinants 141
— , general test of 135
irreducible polynomials 89
isomorphism 57
— of arbitrary systems 70
— , extension of 113

Kakeya's theorem 210
— , generalisation of 237

Lagrange's formula (interpolation) 239
— method for calculating roots 207
— symbols 151
law, associative, commutative and distributive 49, 13 (vectors), 242 (matices)
— of inertia 297
— of inverse existence 49
— of reflexivity, symmetry and transitivity 51
Legendre's polynomials 222
linear equations 8

— — , (non-)homogeneous 20(23)
— — , methods for solving 41
— interpolation 226
— substitution (complex) 274
— transformation 43,251
— — , inverse of 47
loxodromic substitution 274

Matrix 17,242
— , antisymmetric 293
— , characteristic polynomial of 260
— , columns of 17
— , congruent 277
— , conjugate 289
— , diagonal- 46
— , elementary 46
— , function of 29
— , Hermitean 294
— , inverse of 48
— , minor of 35
— , orthogonal 292
— , polynomial in 245
— , rank of 17
— , row of 20
— , similar 250
— , unit- 48
— , zero- 17
— as root of a polynomial 245
minor 35
module 50
monotony of $C(\delta)$ 216
multiple root 107
— — of a characteristic polynomial 262
multiplication 49
— of matrices 45,244
— of polynomials 74
— in a quotientfield 67
— of vectors with numbers (elements) 13(103)

Necessary condition 13
Newton's formula for interpolation 241
— method for approximation of roots 226
non-homogeneous linear equations 23
norm 82
— of a complex number 134
— function 86
normal extension (see : extension, automorphism)
nullelement 56
number 103
— , congruent 51
— , even (odd) 1
— , irrational 198, 195
— , quadratic 177
— , —, reduced 182
— , theory of 127,184
(see also : primenumber)
n-vector 13

Odd number 1
— permutation 6

order of a cyclotomic polynomial 121
original 58
orthogonal matrix 292
— system 27
— vector 20
orthogonalisation 26

Parabolic substitution 274
partition into classes 51
Pell's equation 185
permutation 2
— , composition of 4
— , cyclic 3
— , decomposition of 5
— , even (odd) 6
— , identical 3
— as linear transformation 254
polynomial 72
— , addition (subtraction) of 74
— , alternating 145
— , characteristic 260
— , coefficient of 73
— , cyclotomic 118
— , — , irreducibility of 139
— , — , order of 121
— , — , primitive root of 119
— , degree of 73
— , factorisation of 98
— , homogeneous 79
— , — , degree of 79
— , irreducible 89
— , irreducibility of 135
— , multiplication of 74
— , ring of 74
— , — , commutative 75
— , — , extension of 78
— , — of matrices 245
— , root of 95
— , —, multiple 107
— , separable 108
— , —over a Galoisfield 123
— , symmetric 141
— , — , elementary 142
— , — , homogeneous 143
— , — , main theorem of 144
— , in two indeterminates 77
— of which A is a root 245
Poulain's theorem 227
power series in x^{-1} 186
— sum 147
prime-element 81
— , homomorphism mod. 88
primefield 63
primenumber 87
— $4n+1, 4n+3$ 133
primitive element 110
— root 119
product (see : multiplication, scalar)

Quadratic form 297
— number 177
— — , reduced 178
— residue 128
quotientfield 66

Radical 149
rank (see : field, matrix, vectorspace)
rational function 191
— operation 50
reduction, complete 114
remainder 89
representative 52
resultant 152
ring 55
—, commutative 55
— over a field 103
— of matrices 245
— of polynomials 94
— $R(\Delta)$ 248
— $R(\Delta, n)$ 244
— R_g 60
— $R(K[x],n)$ 284
— $R(J,n)$ 286
row 17
— addition 18
— multiplication 18
— vector 17, 250
— omission 18
root (see : approximation, polynomial, radical)

Scalar 245
— product 26
similar matrices 250
— —, main theorem on 273
skew = antisymmetric
statistical analysis 129
Sturm's theorem 221
subfield 62
subgroup 55
submodule 55
subring 55
subset 55
subspace 16
sufficient 13
sum (see : addition, powersum)
sweep out 17,279
symmetric (see : function, matrix, polynomial)

Taylor expansion 202
tensoralgebra 300
transcendental extension 104
transform of a matrix 250
transformation, linear 42
—, —, composition of 44
—, — representing permutations 254
—, — of vectorspaces 251
—, unitary 292
transposed matrix 250
transposition 3

Uniqueness of the difference 54
— of factorisation 83
— of the quotient 57
— of the singular element 53
unitelement 56
unit-matrix 48
— vector 14
unitary matrix 290
— transformation 292
unity 80

Veblen geometry 129
vector 101, 13 (n-vector)
— , cogradient, contragradient 300
— , column- 17,250
— , dependent 14,103
— , exponent of 267
— , height of 267
— , length of 27
— , matrix representation of 45
— , orthogonal 20
— , — , system of 27
— , row- 17,250
— , scalar product of 26
— , unit- 14
— , zero- 14
vectorspace 14,103
— , basis of 15
— over a field 100
— , rank of 16,101
— R(A) and X(A) 21
— , subspace of 16

Wilson's theorem 127

Zero-element 57
— matrix 17,243
— vector 14.

CORRECTIONS

Page	*Line*	*For*	*Read*
2	25	$\leqq$	$\geqq$
25	head line	non-homogenous	non-homogeneous
38	6	1·9	1·91
61	25	overr	over
	32	hown	shown
64	16	22·3	2·23
80	15	—	2·41 (insert)
	32/33	*commutative*	*abelian*
88	22	$F(x)$	$F[x]$
89	head line	$F(x)$	$F[x]$
127	19	*on*	*to*
128	30	*on*	*to*
129	28	*on*	*to*
147	18	h	h'
	27	s_1	s_m
149	footnote	s	is
150	5	3·54	3·55
	10	3·53	3·55
174	29	*fraction*	*fractions*
206	14	$(x = -q_2)$	$(x - q_2)$
210	28	5·20	5·2
246	6	G	G